PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06	A2	(11) International Publication Number: **WO 00/36807** (43) International Publication Date: 22 June 2000 (22.06.00)

(21) International Application Number: PCT/US99/30139

(22) International Filing Date: 17 December 1999 (17.12.99)

(30) Priority Data:

09/216,388	18 December 1998 (18.12.98)	US
09/216,415	18 December 1998 (18.12.98)	US
09/216,700	18 December 1998 (18.12.98)	US

(71) Applicant: CYBERSIGNS, INC. [US/US]; Suite 202, 8304 Clairemont Mesa Boulevard, San Diego, CA 92111 (US).

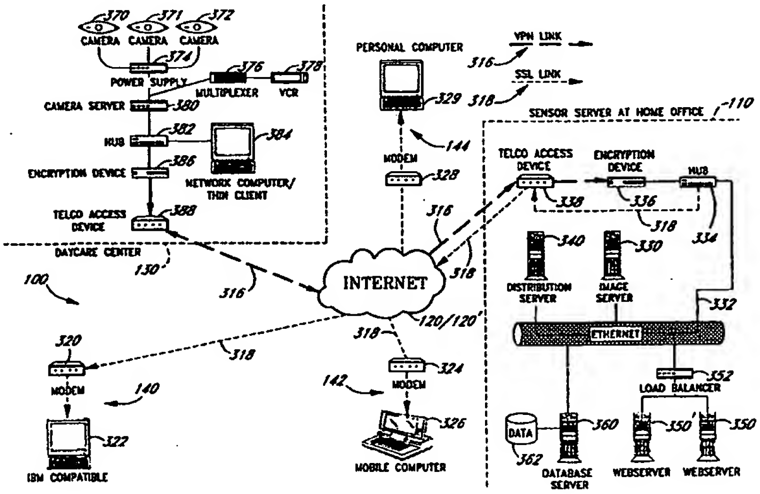
(72) Inventors: BOODMAN, David, J.; 4271 Calle Mar De Ballenas, San Diego, CA 92130 (US). FURMAN, Adam; 11517 Windcrest Lane #38, San Diego, CA 92128 (US). KOZUBIK, John; P.O. Box 4867, Boulder, CO 80306 (US). CHIRANAKHON, Grean; Apt. 183, 3770 Boyd Avenue, San Diego, CA 92111 (US).

(74) Agent: HUNT, Dale, C.; Knobbe, Martens, Olson & Bear, LLP, 16th floor, 620 Newport Center Drive, Newport Beach, CA 92660 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: ENCRYPTED VIRTUAL PRIVATE NETWORK FOR ACCESSING REMOTE SENSORS



(57) Abstract

One aspect of the present invention is directed to a system and method of providing secure access to remote sensor data via an encrypted virtual private network (316). The system (100) utilizes a scaleable architecture and includes a centralized sensor server (110) connected to a plurality of centers (130, 132, 134) having sensors (370, 371, 372) via an encrypted virtual private network. The centralized server also connects to a plurality of remote sensor monitors (140, 142, 144) via a virtual private network. The virtual private network may be implemented over a packet switched network (120) such as the Internet, while the remote sensor monitor utilizes a web browser (520, 522, 524). The system shares images (512) from a particular sensor to multiple users via the centralized server to conserve bandwidth and reduce system costs. The system utilizes various authentication and security features to protect the sensor data.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

ENCRYPTED VIRTUAL PRIVATE NETWORK FOR ACCESSING REMOTE SENSORS

Background of the Invention

Field of the Invention

The present invention generally relates to a system for accessing remote sensors, and more specifically, to an encrypted virtual private network for accessing images from remote cameras.

Description of the Related Technology

In today's world, both parents or a single parent of one or more children must work to support their family. Parents or legal guardians are increasingly concerned about the safety and well-being of their family members or possessions that may be at a day care center, preschool, or other similar facility. Parents also frequently worry about the professionalism of the center employees. A system that would permit a working parent to remotely and securely monitor their children would provide much peace of mind. Such a system should be inexpensive for the parent, easy to use, not require any special equipment or training, and provide security against unauthorized people viewing their children. If a parent is traveling, this monitoring system would allow monitor access of their children from anywhere in the world and also allow relatives that have permission from the parents to also monitor the children. Such access would be via plain old telephone service (POTS), digital subscriber line (DSL), integrated services digital network (ISDN), cable modem or similar connection to the Internet, for example. The use of such a monitoring system by a day care center will provide a competitive advantage over other centers that do not have a child monitoring system.

Several prior monitoring systems utilize "modem cameras" for display of a scene such as a highway, a beach, a ski hill and so forth. These cameras use point-to-point communications rather than a secure centralized system. A user can access the camera by knowing the telephone number associated with the camera and an optional password. Other prior monitoring systems utilize a server that is installed at each day care center. A monitoring system that would utilize a centralized server in communication with a plurality of day care centers so as to conserve system resources would be desired.

Summary of the Invention

The present invention comprises a system and method for monitoring children at a day care center, preschool facility, or other organization by use of multiple video cameras accessed via an encrypted virtual private network. The centers may be accessed by use of POTS, ISDN, DSL, cable modem or other communication channels. The system includes a centralized sensor computing environment which may be embodied as a sensor server or a group of networked servers. The sensor server handles tasks such as user authentication, security, load balancing, and image caching for multiple viewers. A sophisticated viewing system, which includes video cameras that are installed in strategic locations throughout the center, provides images to the sensor server if requested by a remote authorized viewer from anywhere in the world. The viewer accesses the images at the sensor server via an ordinary web browser. Once a parent, guardian or relative has logged into the sensor server and has been authorized, all communication is encrypted for security.

In another embodiment of the present invention there is an encrypted remote monitoring system, comprising a plurality of remotely located sensor networks, each one of the remotely located sensor networks comprising a plurality of sensors providing sensor data; a plurality of remotely located sensor monitors, each one of the remotely located sensor monitors being capable of selectively accessing the sensor data of at least one of the sensors located at a selected one of the remotely located sensor networks; and a centralized sensor computing environment having a first set of connections to the plurality of remotely located sensor networks and a second set of connections to the plurality of remotely located sensor monitors, wherein the first set of connections and the second set of connections form an encrypted virtual private network in a public packet switched network.

In another embodiment of the present invention there is a method of remote monitoring in a system including a centralized server, a plurality of remotely located sensor networks, each network comprising a plurality of sensors, and a plurality of remotely located sensor monitors, the method comprising providing sensor data from at least one of the sensors; communicating the sensor data via an encrypted virtual private network in a public packet switched network to the centralized sensor server; storing the sensor data in the centralized sensor server; and selectively accessing the stored sensor data by at least one of the plurality of remotely located sensor monitors via the encrypted virtual private network.

In another embodiment of the present invention there is an image sharing system, comprising a plurality of image sensors, each sensor being capable of providing a unique sequence of images; a plurality of client computing devices, each client computing device being capable of receiving at least one of the unique sequence of images; an image fetch program in data communication with a selected one of the image sensors, the image fetch program being capable of fetching each one of the images in the image sequence from the selected image sensor; and an image distribution program in data communication with the image fetch program, the image distribution program being capable of distributing the image sequence to selected ones of the client computing devices, wherein the image sequence associated with the selected image sensor is shareably accessed by the selected ones of the computing devices.

In another embodiment of the present invention there is an image sharing system, comprising a plurality of image sensors, each sensor being capable of providing a unique sequence of images; a plurality of client computing devices, each client computing device being capable of receiving at least one of the unique sequence of images; an image server in data communication with a selected image sensor, the image server being capable of generating a sensor thread so as to fetch each one of the images in the image sequence from the selected image sensor; and a distribution server in data communication with an image output of the sensor thread, the distribution server being capable of generating a client data stream for access by a selected client computing device, wherein the image sequence is shared with respect to the selected image sensor by more than one of the client computing devices.

In yet another embodiment of the present invention there is a method of sharing images in a remote monitoring system including a plurality of image sensors and a plurality of client computing devices, the method comprising providing a unique sequence of images associated with a selected one of the image sensors; fetching each one of the images in the image sequence from the selected image sensor; and distributing the image sequence to selected ones of the client computing devices, wherein the image sequence associated with the selected image sensor is shareably accessed by the selected ones of the client computing devices.

In still another embodiment of the present invention there is a method of sharing images in a remote monitoring system including a plurality of image sensors and a plurality of client computing devices, the method comprising providing a unique sequence of images associated with a selected image sensor; retrieving each one of the images in the image sequence from the selected image sensor with a sensor thread; storing the retrieved images of the image sequence in a storage medium; and retrieving the image sequence into a client data stream for shareable accessing the image sequence by selected ones of the client computing devices.

In another embodiment of the present invention there is a method of providing security for a system having a standardized transport protocol server in data communication with a database containing authorized user identification information and a user browser, the method comprising sending a set of connection state data indicative of an authorized user data from a standardized transport protocol server to a user browser corresponding with the authorized user; sending the user connection state data to the standardized transport protocol server when the authorized user selects a link to a secure area of a hyperlinked page; comparing the user connection state data to corresponding connection state data in the database; and granting access to the secure area by the authorized user if the comparison result indicates that the authorized user is permitted to access the secure area.

In another embodiment of the present invention there is a security system for a web application, comprising a web server being capable of sending a web page having at least one secure area; a web database in data communication with the web server, wherein the web database stores connection state data for a plurality of users; a client computing device running a user browser, the user browser being capable of receiving connection state data corresponding to an authorized user from the web server and sending the user's connection state data to the web server when the authorized user selects a link to the secure area of the web page; a security program, executing on the web server, being capable of comparing the received user's connection state data to the corresponding connection state data in the database and denying access to the secure area if the comparison result is negative.

Brief Description of the Drawings

Figure 1 is a top level block diagram of the system configuration of the invention.

Figure 2 is an exemplary screen display seen by a user of the system shown in Figure 1.

Figure 3 is a block diagram showing one embodiment of the hardware components of the system shown in Figure 1.

Figure 4 is a top level operational flowchart of the system shown in Figure 1.

Figure 5 is a block diagram showing the servers, processes and multithreading performed on the sensor server shown in Figure 1.

Figure 6 is a flowchart of a Fetch Images process performed on the sensor server of Figure 1.

Figure 7 is a flowchart of a Dispatch Images process performed on the sensor server of Figure 1.

Figure 8 is a flowchart of the authentication and security aspect performed on the sensor server of Figure 1.

Detailed Description of the Preferred Embodiments

The following detailed description of the preferred embodiments presents a description of certain specific embodiments to assist in understanding the claims. However, the present invention can be embodied in a multitude of different ways as defined and covered by the claims. Reference is now made to the drawings wherein like numerals refer to like parts throughout.

The purpose of the encrypted virtual private network (VPN) for accessing remote sensors is to provide secure images of a child to an authorized parent or guardian located anywhere in the world having access to the network.

The detailed description is organized into the following sections: System Overview, System Topology, Operational Flow and Server Configuration, Fetch Image Process, Dispatch Image Process, Authentication and Security, and Conclusion.

System Overview

Referring to Figure 1, the top-level configuration of a VPN monitoring system 100 will be described. The VPN system 100 comprises two network segments. A first segment 120 exists between a child-care center, such as center 1 (130), center 2 (132) or center N (134), and a centralized sensor computing environment 110 at a central home office location. The centralized sensor computing environment 110 may include a sensor server or one or more networked servers, as will be described hereinbelow. A second segment 120' exists between the sensor server 110 and an authorized viewer at a remote sensor monitor, such as monitor 140, 142 or 144. The links that make up these segments are differentiated in terms of transport and encryption.

In one embodiment, the link 120 between a child care center, e.g., center 130, and the sensor server 110 consists of an encrypted virtual private network run across the public switched telephone network (PSTN). A virtual private network is a network that is transposed on top of another network, but separates itself by means of encryption or other means of security. In this case, the data travels along data lines used for Internet, long distance, etc. but the interception of all or part of the data would not compromise the data since it is secured via encryption. The link 120' between the sensor server 110 and a remote sensor monitor, e.g., 140, also consists of an encrypted virtual private network. Because the system 100 consists of only two links, and because each link is a VPN obscured with very strong encryption, the system 100 is invulnerable to attacks whose goal would be to compromise the system and allow images to be viewed by someone other than the authorized viewer.

Communications between the child care center 130 and the sensor server 110, and between the sensor server 110 and the authorized viewer at monitor 140 are facilitated through the use of a packet switched network such as the PSTN. Information is passed onto the PSTN and taken off of the PSTN through the use of telco access devices, such as routers, DSL modems, ISDN modem-routers, cable modems, and multi-link point-to-point (MLPPP) modems, at the center 130. The telco access devices are often referred to as 'routers' – for instance, a product available from Farallon is called a 'dual analog router'. A telco access device provides an access point from a smaller network at the center 130 to the larger network that is the PSTN. This data that is being passed between the nodes on the system network travels along the PSTN alongside long-distance telephone conversations, corporate data, and data comprising the public Internet. It is possible to safely transmit this data along these semi-public channels because the encryption of the data forms a VPN which cannot be accessed by other users of the PSTN, such as people placing telephone calls, for instance. Because of this, the system 100 isolates the images produced and transmitted only on the secure network, and never on the public Internet. Any mention of 'Internet Viewing' is simply intended as a means to convey the technology to unsophisticated users without confusing them. The only similarity between the technology of the system 100 and 'Internet Viewing' is that both are accomplished with web browsers.

In overview, the system 100 allows an authorized user to ask the sensor server 110 for a current picture, allows the sensor server 110 to fetch that picture from a sensor, e.g., a video camera, at the center 130, and finally transports the requested image from the sensor server 110 to the authorized user at the monitor 140. In another embodiment, the sensor may comprise an infrared sensor, a motion sensor, a sound sensor, a tripwire, and so forth.

In this framework, the sensor server 110 acts as a middleman between the camera and the user. The system 100 is designed such that the camera will only answer requests from the sensor server 110 and will discard the requests of any other entity on the PSTN. The reason for this is twofold. First, by forcing users to authenticate themselves, it is determined that the user is actually an authorized user. In one embodiment, the sensor server 110 uses a three-tier authentication method that forces the user to identify their user name, password (between 8 and 12 characters, letters and numbers), and center identification code. This authentication has an inactivity timeout of a predetermined time interval, such as 15 minutes, and allows the user to choose a camera and view current images from that camera. An inactivity timeout is a function that monitors the user for actions related to the web site (e.g., clicking on a link, viewing a camera, etc.). If none of those actions take place, even if the user is actively using other programs on their computer, the timeout will occur and the user will need to log into the system network again to view a camera.

The second reason to force all users to use the sensor server 110 as a middleman is that it reduces the number of connections that a camera needs to support to one. If users were allowed to connect directly to cameras, each user would make a connection to the camera. This will not work efficiently, since the camera, in one embodiment, is physically limited to receiving only a predetermined number, e.g., five, of concurrent connections. Furthermore, additional network capacity between the center 130 and the link 120 would need to be added at the center 130 to accommodate the increased number of users accessing the sensors in the center. Therefore, the authorized users make their connection to the sensor server 110, and the sensor server 110 only opens one connection to each camera.

The system 100 comprises a web-based application. It is accessible using a standard web browser on any type of Internet connection. Parents and day care staff alike can access the system with their web browser by pointing their browsers to the system home page. Once logged into the system, parents and staff have access to features like message sending, news posts, progress reports as well as images from multiple cameras installed at day care centers. When a center is initially setup, it is provided with a center identification code or school code. This is a code that is unique to each school or organization and is required to login.

The system 100 utilizes an on-line sign-up form for parents so as to capture vital information for advertising purposes and to alleviate the workload for the system administrator. When parents wish to obtain an account, they access the form from the system web page, home page, or hyperlinked page. Such a page may be provided via a hypertext transfer protocol (HTTP). The parents then provide the requested information and answer a few questions on the form. After the form is submitted, they are provided with a temporary password that they can use to access the system once their account is activated. A message is immediately sent to the system administrator (via the "message area") that a new account is awaiting activation. A welcome message is also sent to the new parent's account in their "message area". At this point the account status is "pending" or awaiting activation. To activate the account, the system administrator needs to login and assign a child and cameras to the account. The system then notifies the parent via email that the account is ready. The parent is then free to log onto the system. Initially, they will be prompted to change their temporary password. They will be asked for the temporary password that they received when they signed up and for a new password. The temporary password is determined by the system based on a random selection of one of many pre-designated passwords. For security reasons, the password is delivered to the parents upon completion of the signup form via a secure (SSL) connection to the sensor server.

Parents or staff who wish to log onto their account do so through the system web page. From there, they select the "login" link which will take them to the secured login page. The login page and every page thereafter is served over a 128-bit Secure Sockets Layer (SSL) virtual private network. SSL is an open standard for securing a link between a web server and a web client. A web server may also be referred to as a standardized transport protocol server. At the secured login page, the user is prompted to enter their school code, login name, and password.

Referring to Figure 2, an exemplary screen 200 that is displayed to a parent after login and authorization will now be described. The exemplary screen includes three frame windows; a top left pane 210, a lower left pane 220 and one pane 230 on the right. The top left pane 210 initially presents a tip of the day or an advertisement. Once a sensor is activated, this frame 210 presents images from the cameras. A time and date area 212 associated with the image may also be presented in pane 210. The lower left pane lists a group of sensors, e.g., cameras, available to be viewed by the parent, such as cameras in Room2 (222), Room3 (224), Gym (226) or Playground (228). The right pane 230 is a feature window. Initially, it displays a "News" feature 232. The News feature 232 shows parents general announcements posted by their daycare center staff. Upon logging in, this screen also informs the parents the last time their account was logged into as a security feature. Any unknown login time should be immediately reported to the system administrator and the account password should be reset. The News area also notifies a parent of new messages (a "new messages" message appears). In addition to the "News" feature 232, there are a number of parent features that may be standard with the system 100. These features, which will be discussed further below, are accessible through the exemplary feature icons, e.g., 234-246, that appear at the top of the right pane 230. Note that the location and types of content may vary for each implementation of the system.

When a parent clicks on a camera link, e.g., 222, in the lower-left pane 220, the sensor server 110 (Figure 1) gets images from the selected camera and sends them to the parent's browser as fast as possible. Several factors, including parent's link/modem speed, other Internet applications running on parent's' computers, Internet congestion, Internet Service Provider (ISP) congestion, link speed from the day care center, and other parents accessing the system, all contribute to the speed at which images are delivered to parents. Under optimal conditions, in one embodiment, parents should receive images every two to five seconds. However, the average update time for parents accessing the system over a 33.6 Kbps modem can range from 4-10 or more seconds. The system 100 employs several different delivery models for images based upon which browser the parent is using to access the system. Parents using Netscape version 3.01 and up are delivered images using "server push". This technology (presently supported only by Netscape) sends a constant stream of data to the browser. The browser processes it as a constantly-refreshing image. Clients accessing the system with other browsers are automatically given a Java Applet which automatically loads and reloads images as they become available. Occasionally, cameras may be inaccessible due to downed links or other technical problems. When this happens, parents are given a message that the camera is temporarily unavailable and to try again later.

The icons that appear in the right pane 230 include a mail icon 234, a chat icon 236, a child information icon 238, a preferences icon 240, a links icon 242, a help icon 244 and an exit icon 246. When the mail icon 234 is selected, a screen is displayed that lists the contents of the parents' "mailbox". Messages are listed in reverse chronological order (with the newest messages first). The status of the message will indicate whether the message has been viewed ("read") or has not yet been read ("unread"). The sender and the subject of the message are also listed. To see the contents of a message, the user clicks on the "view" link. Once clicked, the contents of the message are displayed. Parents are then given several options, such as Delete Message, Back to Messages, Reply to Message, Forward Message, and New Message. In one embodiment, messages are transferred inside the system 100 and do not travel to other servers on the Internet. Therefore, it is not possible to send messages using conventional e-mail, i.e., parents cannot send a message to a friend on a public e-mail service. Messages are delivered instantaneously. Once the recipient logs in, he or she is notified of the new message.

When the child information icon 238 is selected, a screen is displayed that provides a convenient way for daycare providers to post information about a child's performance. Daycare center staff will periodically enter information into this area such as "grades" or progress reports. This information is specific for individual children and parents (or authorized viewers) are given access to information about their children. In the case that the 'authorized user' is a grandparent or other relative, the same information that is available to the parent or guardian is also available to other 'authorized users'.

When the preferences icon 240 is selected, a screen is displayed that allows parents to specify certain settings on their account. Initially, the screen displays current settings. Once the desired changes are made, a "Save Preferences" button saves the changes. In one embodiment, several preferences are as follows.

A "Listing" feature allows parents to determine whether or not they want their name to be listed in the "New Message" area. Unlisting causes their name to not appear on the list among other parents. This will a) prevent other parents from knowing that that parent (or their child) belongs to that daycare center; b) prevent other parents from sending them messages. The daycare center staff, customer support, and other service personnel are able to still send messages to unlisted parents. If a parent chooses to be unlisted, they can still send messages to other people, and the recipient will be given the opportunity to reply. However, no one can create a new message to an unlisted parent.

A "Change Password" feature allows parents to change their password at any time. The user enters their old password and new password (they will be asked to type it in twice to confirm). If accepted, the password change takes effect immediately.

A "Change Login" feature allows parents to change their login at any time. The user enters their old login and new login (they will be asked to type it in twice to confirm). If accepted, the login change takes effect immediately.

A "Change Email" feature allows parents to change their email address at any time.

Using the exit icon 246 is the safest and most secure way to exit the system 100. When the exit icon 246 is selected, the browser window is updated and informs the parent that they are being logged out and their browser is being closed. After a few moments, a confirmation window pops up asking them if they want to close their browser. They should then click "yes" and let their browser close, which completes the logout process.

The system web site allows administrators and system personnel to add and delete authorized users, change the cameras at a given center that a user has access to, and generally customize the way that the system is used at a particular center. These procedures are completed by logging into the web site with a user name and password combination that denotes a system administrator. The system administration is done solely through the web site, and allows a system administrator to perform these updates and other tasks from any web browser, anywhere in the world. This feature provides a friendly, familiar manner for the day care personnel to make updates to the system.

System Topology

Referring now to Figure 3 and also Figure 1, one embodiment of the hardware components of the system 100 will be described. As previously mentioned, the system 100 comprises two main network segments. The first network segment 120 consists of the link between a day care center, e.g., center 130, and the sensor server 110. The second network segment 120' consists of the link between the sensor server 110 and an authorized viewer, such as at a computer 322, 326 or 329.

The first network segment 120 begins in the center, e.g., 130. An incoming network connection (such as DSL or ISDN) 316 is connected to a telco access device 388. Exemplary telco access devices include a Paradyne HotWire 5446 DSL modem, model number 5446-a2-200-0rm, a 3Com 56K MLPPP switch, model number 3c430000, and a Netgear ISDN modem, model number RT328. The cabling used in this connection depends on the type of network service being provided. The telco access device 388 is then connected to an encryption device 386, such as a Ravlin-4 wireline encryption device, with a 10-base-T cable. The encryption device 386 is then connected to a hub

382, such as an Ethernet 10-Base-T non-switching hub, with a 10-base-T cable. For most installations, an 8-port hub is sufficient, but considerations such as center size, expansion, and so forth may dictate a 16-port hub or larger. The hub 382 is connected to a network computer/thin client device, such as a network computing device (NCD) 384, which includes a Microsoft Windows-based network computer running a compatible browser. The hub 382, in turn, is also connected to one or more camera servers 380 (remote sensor servers) such as the Axis model 240, or Axis model 200/200+ cameras, with 10-base-T cable(s). Each of the Axis camera servers 380 connects to a power supply and media aggregator device 374 via RCA type cables, in one embodiment. Each of the cameras 370, 371, 372 connects to the media aggregator 374 with a 75 ohm coaxial video cable. In one embodiment, the camera may be an auto-iris solid-state color camera, with a 6mm lens utilizing 12 volt DC power. The media aggregator 374 optionally connects to a multiplexer 376, such as an Advanced Technology model DPX16, with an RCA-type cable. The multiplexer 376 further connects to a video cassette recorder (VCR), such as a Sanyo SRT-768, with an RCA-type video cable. The above architecture describes the 'day care center network'. Of course, one skilled in communication technology could substitute other hardware devices or utilize software to perform some of the above tasks, e.g., the encryption.

Important aspects of the physical topology include the following:

- The use of encryption devices 386, 336 between the center 130 and the sensor server 110. This ensures that all data traffic passed on the segment 120 via the PSTN from the center 130 to the sensor server 110 is completely secure and forms a VPN connection 316 using a 168-bit triple DES encryption level. Other types of encryption may be used in another embodiment. Of equal importance, the encryption devices 386, 336 ensure that the cameras, e.g., camera 370, cannot be contacted in any way by anyone on the PSTN except by the computers at the location of the sensor server 110.
- The cameras, e.g., camera 370, are connected to the power supply and media aggregator device 374 with video cable. This cable allows the camera 370 to transmit its video images to the device 374 and further to the camera server 380. However, the power to run the camera is passed through this same video cable as well, and permits installing the cameras at a center 130 without running separate lines for power and video. In addition, audio is supported on these cables as well as video and power. However, in one embodiment, the camera servers 380 do not utilize the audio capability.
- Because the camera servers 380 are connected directly to the hub 382 which is connected directly to the PSTN (through the encryption device 386 and the telco access device 388), no computer is necessary at the center 130. The center network is set up and functions without a computer. The camera server 380 is known as a "thin" server and is not a computer. The camera server 380 comprises a processor and memory, but does not include a keyboard or pointing device, a video display device nor a mass storage device, e.g., a hard disk drive. A "thin" server provides network connectivity for non-personal computer devices, such as video cameras.
- The network computer 384 at the center 130 is provided for convenience in accessing an administration system (not shown). It is not necessary for the operation of the system to deliver images. The network computer 384

has no moving parts and is controlled directly from the sensor server 110. It is not user configurable, but is given its configuration from the computers at the sensor server location (at the home office).

- The encryption device 386 at the center 130 is remotely configurable from the location of the sensor server 110.
- In another embodiment, a Microsoft Windows based personal computer may be used in place of the network computer 384. Individual Axis model 200 or model 200+ cameras that can be wired directly to the hub 382 (with 10-base-T cable) may be used rather than using the camera server 380 and media aggregator 374. If the hub 382 can be wired directly to an existing incoming Internet connection, the telco access device 388 may be deleted from the center network.

The center network at the center 130 is connected to the 'sensor server network' through a combination of Public Switched Telephone Networks and private business data lines. The particular combination is not important, and is administered entirely by one or more Regional Bell Operating Companies, Long Distance Carriers, etc.

The second network segment 120' begins at the sensor server network. The second network connection comes from the same PSTN and leased data line cloud that the outgoing center network is connected to. This second network connection is connected to a telco access device 338, which is in turn connected to the encryption device 336 with a 10-base-T cable. The encryption device 336 is then connected to a switched-hub 334 with another 10-base-T cable. The hub 334 is further connected to a sensor server network 332, such as a Fast-Ethernet network. The incoming data traffic flows on the second network segment in the order outlined above.

The outgoing data traffic travels a similar course, but in reverse: from the sensor server network 332 to the hub 334, and traveling through the encryption device 336. The outgoing data travels through the encryption device 336 in an unencrypted form when the data is not headed to a center, e.g., center 130. When data flows to one of the remote sensor monitors 140, it is encrypted by software via a 128-bit SSL connection 318 and travels out to the PSTN and leased data line cloud. Hence, the virtual line 318 indicates that the encryption device 336 passes the outgoing data traffic transparently to the telco access device 338. 128-bit SSL is currently the strongest level of this encryption supported by most major browsers. Other levels or types of encryption may be used in another embodiment. The destination of this outgoing traffic is the authorized viewers at the remote sensor monitors, e.g. 140. Authorized viewers may connect to the PSTN and leased data line cloud through any number of means – using their Internet service provider, using a private corporate network, or connecting directly through a long distance carrier such as MCI or Sprint. Of course, one skilled in communication technology could substitute other hardware devices or utilize software to perform some of the above tasks, e.g., the encryption.

The sensor server network 332 may include one or more servers to facilitate operation of the system. The sensor server network 332 may include one or more web servers 350 to service incoming requests from a remote sensor monitor, e.g., monitor 144. The monitor 144 may include a browser running on a client computing device such as a personal computer 329 that connects to the segment 120' via a modem 328 using the SSL link 318. The monitor 140 may include a modem 320 and an IBM compatible personal computer 322, and the monitor 142 may include a modem 324 and a portable computer 326. If more than one web server is utilized by the network 332, a load balancer

352, such as a RADWare WSD Pro, interfaces the web servers, e.g., servers 350, 350', to the network 332. The sensor server network 332 may also include an image server 330 to obtain images from the center 130, a distribution server 340 to provide the obtained images to an authorized user, a data storage or database 362 for storing the obtained images, authorization data and other related information, and a database server 360 for storing and accessing data in the data storage 362. The accessed data is utilized by the web server 350, the image server 330, and the distribution server 340.

The system 100 is designed to be easy to use, and require little or no training or special software to operate. Therefore, the system works over any Internet connection, using any number of web browsers. Although the goal is to support every make and version of browser, in one embodiment, browsers accessing the system support the following features:

- Frames - browser window can support frames, creating panes that can contain independent information.
- SSL 2.0 - a secure TCP/IP transmission standard created to allow secure data transmissions between servers and browser clients.
- Java or server push - Browsers that are Java compliant will be able to run Java Applets. Applets are a type of plug-in that runs and functions within a browser. Clients that support server push (e.g., Netscape) do not need to support Java.

Browsers that have been tested include Netscape 3.01 and up, Microsoft Internet Explorer (MSIE) 3.0 and up, and MSIE 3.0 for America Online (AOL). Static (non auto-updating) images are presented to users accessing system 100 with WebTV. Although almost any speed modem is sufficient enough to connect to the system 100, it is recommended that parents use at least a 28.8 Kbps or faster modem, e.g., modem 320. Slower speed modems will result in slow image updates.

Accessing the system 100 via the Internet does not requires a special Internet connection. An ordinary user account from an ISP that allows Internet access is sufficient. Companies such as AOL, Microsoft Network (MSN), Earthlink, Mindspring, IBM Internet, Netcom, or others provide this service to thousands of users. However, not all ISPs provide equal service. Many factors may influence how fast data (images) get delivered from the system servers to the parent. Users at large ISPs may suffer from bottlenecks due to the large amount of users competing for a limited amount of available bandwidth.

Operational Flow and Server Configuration

Referring to Figures 4, a top-level operational flow process 400 of the system 100 will be described. The servers, processes and threads used by the operational flow process 400 are shown in Figure 5, which will also be referred to in this description. Beginning at a start state 402, process 400 moves to state wherein a user accesses the system web site by typing the world wide web address for the system 100 into their web browser, e.g., user browser 2 (522), which is running on the user's client computing device, e.g., computer 329 (Figure 3). Line 526 shows this request and a response by one of the web servers, e.g., web server 350, of the sensor server 110 (Figure 3). The request and the response, which is information that comprises the web site home page, are transferred via segment 120' (Figure 1). The user can choose to leave the web site at state 406 and complete process 400 at end state 408 or to browse informational areas of the web site at state 410. The user can click on any link on the home page to view the information that that link points to, however, one link (the 'parent login' button) takes the user into an authentication mechanism, and ultimately, into the secure portion of the web site. When the user clicks on the 'parent login' button, process 400 proceeds to state 412, wherein the web server 350 responds, in one embodiment, by initiating a secure 128-bit SSL connection with the browser 522 running on the client computing device and generating a login screen with spaces for center code, user name, and password.

The user responds at state 412 by providing the data needed to perform authentication, e.g., center code, user name, and password, which are sent to the database server 360 on line 528. The database server 360 then accesses the database 362 by the center code. The database server 360 checks all of the user name and password combinations for that particular center and looks up the user name that the user entered. Proceeding to a decision state 414, the password is then compared. If the user-entered password does not match the password in the database 362, process 400 advances to a decision state 416 to determine if the user has reached the limit for trying to enter the authentication data. If not, the user is allowed to try again at state 412. However, if the user has reached the limit for trying to enter the authentication data, as determined at decision state 416, process 400 continues at state 418 wherein the user is logged off the system web site and the process 400 completes at end state 408.

Returning to decision state 414, if the user name and password match the user name and password in the database 362 for the particular center, process 400 moves to state 420 wherein the user is authorized for the secure portion of the web site. If the time interval since the date of the last password change exceeds the time allowed for a user to keep a single password, the web server 350 prompts the user to change their password. The web server 350 then requests the database server 360 to check the database 362 to obtain a list of camera names that the particular user is allowed to view at the center identified by the center code. Proceeding to state 422, the web server 350 generates a web page with three frames as seen in Figure 2. Frame 230 contains all of the support links (such as child information, preferences, chat, etc.). The top-left frame 210 contains the space for a video image to be displayed, and the bottom-left frame 220 contains a list of all of the cameras names that the user has access to view.

Moving to state 424, when the user clicks on one of the camera names in the bottom-left frame 220, the web server 350 sends a user request to the image server 330 via line 530 to initiate a connection with the selected camera. Proceeding to function 430, the image server 330 portion of the sensor server 110 instructs the selected camera to transmit the most current image. The most current image is then placed in a directory in the data storage 362 on the data server 360. In another embodiment, the current image may be alternatively placed into a data storage device on the image server 330.

It is important to note that a connection is made between the distribution server 340 and the browser of the authorized user only when a new current image is received from the camera into the data storage 362. In one embodiment, the image is sent from the distribution server 340 to the user via the web server 350. In another embodiment, requests may be sent directly to the image server 330 and sensor data returned by the distribution server 340 to the user browser, e.g., browser 522. In this manner, bandwidth is preserved and connections are only made on each of the two links of the system network when necessary. The most current image, e.g., image 512, is then transmitted from the data storage 362 to the web browser 522, of the user's computing device. If more than one user is trying to view images from that particular camera, the image server 330 does not contact the camera additional times, but rather the distribution server 340 just establishes more connections between the data storage 362 and the authorized viewers. In this way, only one connection is ever made with the camera even if several users are viewing the particular camera.

If the image server 330 senses a problem with a camera during the transmission of the images from the camera, the image server 330 pauses the image transmission and uses the Telnet protocol to contact the camera and reset it. After allowing time for the camera to reset, the image transmission resumes.

Advancing to state 432, process 400 waits for a user action, such as clicking on a different camera name in the frame 220, or for a user timeout. Proceeding to a decision state 434, if the user does not click any links, buttons, cameras names, or so forth on the web page for a predetermined time interval, e.g., fifteen minutes in one embodiment, process 400 moves to state 436. At state 436, process 400 informs the user that their inactivity has caused the system 100 to disconnect them. To continue using the system at this point, the user must log in again. Note that in one embodiment, a particular camera may have a different timeout period, e.g., five minutes, than the user timeout for lack of user activity. Of course, the user timeout interval and the camera timeout interval can be set to other time values as determined by a home office administrator.

Referring again to Figure 5, the servers, processes and threads will now be further discussed. The problem of collecting images from cameras in the field, and distributing them efficiently to remote web browsers in such a manner that the facilitating equipment (i.e., the servers in the middle) can be scaled easily and economically has not yet been solved in the marketplace until this invention. The solution to this problem includes splitting the sensor server 110 (Figure 1) into several portions or duties, each of which may be represented by a process that resides on an individual server. The following discussion describes how the application has been split into four portions, and how these four portions run on the individual servers.

To collect and serve images from a center efficiently, four duties are performed. First, the web server 350 is used to display the system home page and collect the input of users clicking links on the home page. Second, a program or process, which runs on the image server 330, is used to fetch images from the cameras and deposit them in the data storage 362. Third, a program or process, which runs on the distribution server 340, is used to take the deposited images and distribute them to authorized viewers. Finally, the database 362, which is accessed by the database server 360, is used to provide authorization data and user information to all of the other servers. The web server 350 queries this database to determine which cameras a parent is allowed to use, and verify login information such as user names and passwords. These are the four portions of the sensor server 110.

Although it is possible to run these four portions (servers) at the same time on one individual computer, this is inefficient and very intensive on such a computer. Instead of using a single computer, the system 100 was developed to operate the four aspects independently and enable communication with each other using a computer network. In this manner, each portion runs on a separate machine, for a total of four computers. The unique solution to the problem of efficiently and securely conveying images from cameras in the field to remote users with browsers, is the division of the problem into these duties, and the placement of the duties among the servers of the sensor server 110. In one embodiment, four servers are used. Of course, one skilled in communication technology could utilize different partitioning to perform some of the above duties.

To clarify how these servers work together, the following discussion describes what happens, and what interactions take place, when a user attempts to use the system web site. First, a user at a remote location brings up their web browser and types in the web address of the system home page. This action causes the web server 350 to send a copy of the home page. Next, the user clicks on a link leading to a "login" page that prompts them to enter their center code, user name and password to log into the system web site. This action causes the web server 350 to query the database server 360. Presuming the database server 360 affirms that the user name and password are valid, the web server 350 sends a page to the user's browser that allows the user to select and view images from one of the cameras at the center identified by the center code. On this page, the user selects a camera link. The web server first checks with the database server 360 for a list of the camera names accessible by the particular user and just displays those camera names on the lower left pane of the page. The web server 350, after receiving the request for a particular camera link, checks with the database server 360 to confirm that the particular user has access to that camera. If so, the web server 350 then initiates image retrieval by a request to a sensor process at the image server 330, while, at the same time, initiating image distribution by a request to a user process at the distribution server 340. Upon initiation, these two servers 330, 340 check with the database server 360 (via line 532 for the image server and not shown for the distribution server) to see how long they should run before terminating, and will then proceed to fetch, deposit, and distribute images until the expiration time. The web server 350 watches for the processes on these servers 330, 340 to expire. When the processes expire, the web server 350 then takes over again and displays a time-out message or a general information message in the top-left pane 210 (Figure 2) in place of the images from the center.

By splitting the application into four pieces, hardware can be applied to the system where it is needed most. For instance, given four servers that have the same specifications, one server might run the web server at a speed sufficient to serve 100,000 clients per day, and one might run the database server at a speed sufficient to serve 10,000 clients per day. If all four processes were together on one server, to support enough database connections for 100,000 clients per day, a server would be needed that was capable of also serving 1,000,000 web clients, which is ten times more powerful than is necessary. By use of the four servers, a particular server is upgraded only as necessary, and the other servers may be unchanged because they are separate entities on separate machines. This system architecture provides great scalability and is more economical in terms of applying increased computer power only where it is needed, and never wasting computing resources.

The sensor server 110 (Figure 3) serves images to parents at remote locations, and collects images from cameras installed in day care centers. These two tasks are completed with separate programs or processes – a program that fetches the images from a day care center, and a program that dispatches the fetched images to clients using web browsers. These two programs each reside on separate servers that are linked with a network, although, in another embodiment, can reside simultaneously on one server.

Fetch Images Process

Referring to Figure 6 and also to Figure 5, a Fetch Images process 600 will now be described. The process 600 that fetches images requires three things: a stimulus to begin fetching, a camera to fetch from, and a storage medium to place the images, once fetched. An example of a stimulus that would cause process 600 to begin fetching would be a user clicking on a sensor link on a web page, or a clock reaching a preset time. Cameras from which to fetch images are located in day care centers 130 (Figure 1) in remote locations that are accessible by the process through the computer network 120. An example of the data storage 362 (Figures 3 and 5) in which to store the images would be a disk drive residing on the data server 360.

In one embodiment, the image server utilizes the Microsoft Windows NT Server version 4 SP3 with Internet Information Server (IIS) version 4.0 operating software. The process 600 is written in the Java, perl, and C++ programming languages.

Process 600 is running on the image server 330 at all times – it has no dormant, or inactive mode. Beginning at a start state 602, process 600 moves to state 604 where a stimulus to begin fetching an image is received. Advancing to a decision state 606, if process 600 receives a stimulus to begin fetching and depositing images from a camera that already has a previous, un-expired thread that is fetching images, it will not duplicate the effort. Rather, it extends an expiration time (sensor timer) of the existing thread at state 612, and then proceeds to state 614 to access the selected sensor. In this way, no matter how many users attempt to view a specific camera, only one thread is actually transferring the images. If the specified camera is not already active, as determined at state 606, process 600 continues at state 608 and spawns a sensor thread, e.g., thread 1 (550) for sensor (1) 370 (Figure 3), thread 2 (552) for sensor 2 (371), or thread N (554) for sensor N (372), to match that stimulus. That sensor thread services the camera/sensor whose address is specified in the stimulus. Moving to state 610, process 600 sets the sensor timer to a predetermined time and activates the sensor timer. These actions describe reacting to the stimulus not by fetching and depositing a single image, but rather by fetching and depositing images for a set amount of time. In this manner, the process receives the stimulus (for instance, a user clicking a link on a web page) and spawns a thread that would fetch and deposit images for 5 minutes, for example. At the end of the five minute period, the thread would terminate.

Proceeding to state 614, process 600 accesses the selected sensor, and then at state 616, fetches the image and places that image, e.g., image 512, in the data storage medium 362. Moving to a decision state 618, process 600 determines if a user action has occurred, such as clicking on a different sensor link. If so, process 600 proceeds to state 606 to determine if a thread for the newly selected sensor is already active.

Process 600 is multi-threaded. This means that if two such stimuli are received, two separate instances of the process are not needed to facilitate fetching and depositing to satisfy the two stimuli. Rather, a separate thread is spawned from the single instance of the persistent sensor process that is running on the image server 330, each satisfying one stimulus by fetching images from the specified camera and depositing them in the specified directory. The number of threads that can be simultaneously spawned (and which will expire after a set period of time, or, in another embodiment, immediately after fetching and depositing one image) is limited (practically) by the speed of the computer that the process is running on. The number of images that a specific thread can fetch and deposit before that thread times out is limited by the speed at which the image can be transmitted from the camera to the computer.

Returning to decision state 618, if it has been determined that there is no new user action, process 600 advances to a decision state 620 to determine if the sensor timer has expired. If so, process 600 moves to state 624, terminates the spawned thread and then waits for another new stimulus at state 626. When a new stimulus (e.g., user request 530) is received by the image server 330, process 600 continues at state 604 as described above.

Returning to decision state 620, if it has been determined that the sensor timer has not expired, process 600 moves to a decision state 622 to determine if the distribution server 340 is still providing images to the user browser. If no one is requesting the images at the client browser, process 600 terminates the thread at state 624. However, if the distribution server 340 is still providing images to the user browser, process 600 moves to state 614 to get another image from the selected sensor.

After all threads have timed out and no additional stimulus is received, the number of active threads is zero, and the program will (once again) not be fetching or depositing any images in the data storage 362. At this time, process 600 is waiting for a new stimulus.

In one embodiment, the image server 330 makes a connection to the camera at the day care center using the hypertext transfer protocol (HTTP). If a connection cannot be made, it will wait a specified interval (that can be easily changed) and try again. If it fails a predetermined number of times, it will discontinue its efforts after first displaying one image to the user informing the user that the camera is down. If the camera is not down, however, the image server 330 requests the most recent picture taken by the camera – this request is also made using HTTP. When the requested image is received, it is placed in a specified directory in the data storage 362. After the image has been placed in the specified directory, process 600 waits a specified amount of time and then repeats the process, but this time, in one embodiment, deleting the existing image in the directory before placing the new one there. In another embodiment, the system names each image as a new one is brought in, and saves the images until a command is issued to stop saving the images. If at any stage of this process the image server 330 receives an image of size zero, or cannot successfully log in to the camera using the predetermined login name and password, it will attempt to log in to the camera using the Telnet protocol and issue a reset command. This usually cures the camera of any problems it might be having.

Dispatch Images Process

Referring to Figure 7 and also to Figure 5, a Dispatch Images process 700 will now be described. The process 700 is a persistent user process running on the distribution server 340. In one embodiment, the distribution server 340 utilizes the Microsoft Windows NT Server version 4 SP3 with Internet Information Server 4.0 operating software. The process 700 is written in Java, perl, and C++ programming languages.

While process 600 (Figure 6), which fetches and deposits images, is running, process 700, which dispatches images to remote clients (users with web browsers), is also running. Process 700 also receives a stimulus from an outside source, i.e., a request from the web server 350. Process 700 responds to this stimulus by taking the most recent image from the depository area of data store 362 that the fetching program dumps its images in and sending it to the remote client.

Like the fetching process 600 running on the image server 330, process 700 runs on the distribution server 340 at all times – it has no dormant, or inactive mode. Beginning at a start state 702, process 700 moves to state 704 wherein the distribution server 700 receives a request to dispatch an image to a user browser. Process 700 responds to the stimulus by spawning a client data stream, e.g., client data stream 1 (556), client data stream 2 (558), or client data stream M (560), that sends or transports either one image to the remote client, or multiple images until a time period expires. If more than one stimulus is received, more than one client data stream is spawned, each servicing the stimulus that spawned it until the client data stream expires.

Moving to state 708, process 700 sets a sensor timer to a predetermined time, e.g., five minutes, and activates the timer. Proceeding to state 710, process 700 accesses the image for the particular sensor selected by the user, e.g., image 512, in the data storage 362, which was provided by the fetch process 600. Advancing to state 712, the accessed image is sent to the user browser, e.g., user browser 2 (522), for display on the client computing device, e.g., computer 329 (Figure 3). Proceeding to a decision state 714, process 700 determines if the remote user has stopped using the process 700, for instance, if they close their browser. If so, process 700 proceeds to state 718 and notes that it has nowhere to send the image, and therefore stops sending the images by terminating the client data stream. Further, if the user has not closed their browser, as determined at state 714, process 700 continues at a decision state 716 to determine if the sensor timer has expired. If not, process 700 waits for the next image to be available in the storage 362 for the particular sensor and accesses that image at state 710, as described above. If the sensor timer has expired, as determined at state 716, process 700 proceeds to state 718 to terminate the client data stream.

If process 700 determines that no client data streams anywhere are serving the specific images to remote users, and determines that the fetch process 600 is still fetching images for these non-existent users, rather than allow the fetching and depositing to continue until the timer expires (in process 600), the dispatch process 700 moves to state 720. At state 720, process 700 sends a message to the image server 330 (on line 534) to terminate the relevant thread of the fetch process 600. If no user is looking at images from a specific camera, the fetching and depositing thread of process 600 is not allowed to continue to run. Process 700 ends at an end state 722.

The number of client data streams spawned by process 700 is equal to the number of remote viewers that query a camera for images. Unlike the fetch process 600 that fetched and deposited images from a camera with one thread, regardless of the number of users querying the camera, process 700 runs a single client data stream for every user, because each user needs their own stream of images sent directly to their specific browser address.

In one embodiment, process 700 watches the specified directory in the storage 362 that the fetch process 600 is writing images into and sends every new image it finds there out to the end user. If there are fifty end users at a particular time, for example, process 700 will make fifty separate connections for the end users, whereas the fetch process 600 still only makes one connection to each camera. Finally, process 700 does not send an image to a user unless it is a new one – it sends an image only when a new image is fetched by the fetch process 600.

Authentication and Security

The system 100 is an Internet-based application providing authorized users with the capability to remotely view children in day care centers and other facilities. The nature of the information being transmitted requires certain measures to ensure only authorized users are able to access the system (including images of the children). Given the broad range of web-browsers and Internet Service Providers, special steps are taken to ensure uniform security measures across all browsers on all platforms.

Referring to Figure 8, an authentication and security process 800 will now be described. To gain access to the system 100, a parent or other user utilizes their web browser, e.g., browser 522 (Figure 5), to connect to the system web site. Beginning at a start state 802, process 800 moves to state 804 wherein a login page asks for a school or organization code, a login name, and a user password. From this point forward (until logging out), all communications between the user's browser and the sensor server 110 (Figure 3) are sent using SSL. Once submitted, the entered login name and user password are compared against the data in the database associated with the database server 360 (Figure 5) for an exact match. If there is no match, process 800 advances to state 808, refuses further access to the user and an error message is provided to the user. If the match is valid, process 800 proceeds to state 810 wherein the user is considered 'authorized' and is permitted to access the secure area of the system web site.

Moving to state 812, one of the web servers 350 (Figures 3, 5) sends a "cookie" to the authorized user's browser. A cookie, which may also be referred to as "connection state data", is a set of information stored in a web browser that is used to identify a user to a particular web server. In one embodiment, the cookie contains basic information about that user's account including the school identification (ID), their account ID, their child (or children's) account ID, what browser they are using, a random and unique code, and an expiration time and date for that cookie. All information is in a coded form and identifying information is not placed in the cookie. Immediately after the cookie is sent to the authorized user's browser, process 800 advances to state 814 wherein the user is seamlessly sent to the 'private/secure' area of the system 100 where all the features and viewing are accessible. The private area is only accessible to users with a valid user name and user password. In one embodiment, an authorized user can selected one of a plurality of secure camera/sensor links to access images of their child. Proceeding to a decision state 816, process 800 determines if the user has selected a link to a secure area of the web site, e.g., a camera link. If not, process 800 moves to state 818 wherein a non-secure task is performed, such as when the links icon 242 (Figure 2) is selected. However, if the user has selected a link to a secure area of the web site, as determined at state 816, process 800 proceeds to state 820 wherein the user cookie is presented by the web browser 522 to the web server 350.

Due to the nature of web browsing, information pertaining to a unique transaction between a browser and the web server are discrete communication events. Each 'click' (leading to a new page) constitutes another transaction (or set of transactions) that the web server processes as unique and unrelated events. This presents a problem to web publishers who wish to carry information from one screen to another. Most of this problem is solved through the use of hypertext markup language (HTML) forms, but restricting access is a larger problem. To ensure security, each connection to the web server must be validated before information can be sent to the user's browser. Web browser companies have provided built-in mechanisms to take a user name and user password from users. In this scheme, the user name and password are sent to the server (along with the request) every time the browser accesses the server. This can pose a security problem since it inherently increases the number of times the user name and password are transmitted back and forth across the Internet, and hence the larger probability that someone could intercept and crack that user name and password. The other pitfall of this scheme is a loophole that allows users to use the 'back' key on their browser to get back into 'secured' or 'private' areas of web sites. An example of this would be a user who was conducting on-line banking and then wished to 'exit' their account by simply typing in a uniform resource locator (URL) for another web site. If that user or an unauthorized user were to click the 'back' button on the browser, they would eventually find themselves back in the 'private' area, free to conduct business or other devious tasks.

System 100 circumvents this potential loophole by utilizing specially-designed cookies. Every time an authorized user clicks on a link to access any secured or private part of the system 100, the user's cookie is presented by the web browser to the web server at state 820. Advancing to state 822, the web server immediately processes the contents of the cookie and compares the contents to data stored in the database associated with the database server 360 (Figure 5). Information such as the ID of the user and the random unique code are compared to the database for validity. Continuing at a decision state 824, if a match is not found, process 800 moves to state 826 wherein the user is presented with a failure message and service is refused. If the cookie data is valid, as determined at decision state 824, process 800 advances to a decision state 828 to determine if the user has been inactive in the web site for a preselected amount of time. If the user has been active in the web site within the time interval, process 800 proceeds to state 830 and transmits the requested data to the user browser. Advancing to a decision state 832, process 832 determines if there has been a user action in the web site. If not, process 800 moves back to decision state 828 to see if the timeout interval has been reached. If there has been a user action, e.g., the user has clicked on a link or icon, as determined at decision state 832, process 800 proceeds through connector A (834) to decision state 816 to process the action as described above.

If an authorized user, after logging in to the system 100, chooses to visit another web site and, after the preselected time interval, e.g., 15 minutes, uses the 'back' key to return to the system web site, they will be refused access. In addition to comparing the random unique code and ID contained in the cookie, the web server 350 also looks in the database associated with the database server 360 to determine the expiration time for a user login. If, after matching up all the cookie data to the database, everything matches but the login time has expired, the user is refused further access and explained that their login time expired due to inactivity at states 840 and 842. In one embodiment, the inactivity time setting in the database is determined by incrementing the setting 15 minutes into the future every time the authorized user accesses the system 100. If that user does not have a user action in the system web site, or visits another site and comes back to the system web site 15 minutes later, the process 800 recognizes that the login session has 'expired' and that the user needs to log in again.

If a user visits another site on the Internet and then uses their 'back' key to return to the system web site within the preselected time, e.g., 15 minutes, they are able to view the secure/private areas of the system and click on sensor links. The act of clicking on a sensor or other link at that time would increment their inactivity time by 15 minutes into the future. However, if they were to click the 'back' key to get back into the system web site, and then failed to click on any link within 15 minutes from the last time they clicked a link, an attempt to click on any secured-content link would then result in an inactivity timeout as determined by the process 800 at decision state 828.

The technology employed in this security measure ensures that authorized users using a cookie-enabled web browser experience a high-level of security and user authenticity. The system 100 makes use of standard browser features in a unique fashion. Users who don't enter a valid login name or user password are not issued a cookie from the web server, and therefore are unable to access any of the secure system content.

The system 100 includes various other security features. Some of the features making the system secure are in place and function regardless of user intervention. However, some other features, such as granting parents access to cameras, and granting accounts, require staff members and the system administrator to adhere to certain rules. Some of these features and rules are as follows:

- Unique Login Name and Password - Each parent chooses a unique identity to access the system web site. This ensures that only authorized individuals can access the system. In one embodiment, login or user names contain between eight and twelve letters, and passwords contain a combination of letters and characters between eight and twelve characters long. This increases the difficulty for someone to guess the login and password. If a user's login or password does not meet the minimum requirements, they will be requested by the system to input a valid entry.
- Password Rotation - Each registered user is forced to choose a new user password every two months, thereby increasing the difficulty for anyone attempting to hack into a parent's account through brute force. Of course, other time periods can be utilized.

- Restricted Access - Only parents with children enrolled in a system child care center are issued an account to access that center's cameras for viewing. Also, access to cameras is limited to parents who have children in the room where the camera is installed.
- Encrypted Transmission - In one embodiment, information sent from the system servers to the parent, is encrypted using a 128-bit Class 3 SSL. This encryption type is currently one of the highest levels of encryption permitted by the United States. This is the same level of encryption that U.S. banks use to do web-commerce.
- Cached Memory Cleared - The information on a web page doesn't remain on a user's computer's memory after exiting the system, thereby eliminating the possibility of anyone accessing the images from the computer that a parent had been using.
- System Intelligence - The system informs each user when he or she has last logged onto the network, alerting him or her if there have been any unsanctioned logons.
- Automated System Termination - Prohibiting unauthorized access to the system from a parent's computer while he or she is away, the system automatically logs each account off after a preselected time interval, e.g., 15 minutes, of inactivity. This is also reassuring to employers who do not want their employees constantly logged into the system watching their child for the entire work day.
- Center Identity Undetectable - Avoiding the possibility of anyone determining what child care center each child is in, center identity and location is not revealed by the system.
- User Anonymity - The system offers the choice for a person to keep their identity undetectable to other parents who are also using the system at their day care center.
- User Control of Passwords and Login Names - Each parent, or other authorized user, has the ability to reset their password or login name as well as the ability to choose a unique sequence to make it easier to remember.
- Center Staff Controls Access - Parents request additional accounts giving the center staff the ability to determine appropriateness of access for the additional users as well as the ability to regulate the number of authorized users.

Conclusion

Several aspects of the above description are unique to the design and implementation of the system, and are summarized as follows:

The ability to show images from the same camera to multiple users while only one connection is made to the camera from the server is made possible by using the sensor server at the home office as a middleman. This conserves bandwidth between the home office and the child care center, and ensures that the number of parents that can simultaneous access images from one particular camera is limited only by the bandwidth between the home office and the authorized user.

The system design ensures that bandwidth between the home office and the authorized user is also conserved as an image is only sent to the user when a new image is received by the sensor server from the camera, rather than a system that transmits the image from the server at a specified interval, regardless of whether the image has actually been updated from the camera.

The sensor server, after determining that the user has entered a valid login and password, checks the database again to determine which of the cameras at that particular center the user has access to. In this manner, parents can be given access to all of the cameras at a center, or only a subset of the cameras at the center.

If the sensor server ever senses that a camera is not responding correctly, a diagnostic measure is taken by logging into the camera via the Telnet protocol and resetting the camera. In this manner, the cameras can be fixed if they stop functioning, and this fixing does not involve human interaction. In most situations, this is not noticed by the user accessing the camera in question.

If the user does not produce any activity (such as clicking a link, etc.) for the preselected time interval, e.g., 15 minutes, the user's particular 128-bit SSL connection is terminated and they are presented with a new page that allows them to log in again. This provides the system an added measure of security by disallowing the user from leaving their session unattended and potentially allowing an unauthorized user to view images.

The user cannot leave the system web site once a secure 128-bit VPN has been established and then use the browser's 'back' button to return to the session if the 15 minute inactivity time-out has elapsed. This is in contrast to many on-line banking applications on the web that establish a secure connection, and allow the user to come and go in and out of that secure connection at will. This is an added security measure, and ensures that if the user leaves the secure connection for an extended period, they cannot come back unless they log in again.

In one embodiment, the passwords are required to be between 8 and 12 characters long with upper and lowercase letters, and numbers. This makes for very strong passwords that cannot be easily guessed. In addition, only one person can log on with a given user name at a time.

A particular child care center is determined when the user enters the 'center code' but at no time is the center actually identified by name, nor are the actual network addresses of the cameras revealed. This makes it difficult for an unauthorized user with unsavory intentions to determine where the children they are looking at are located.

The processes that run on the sensor server and deliver the images to clients and fetch the images from cameras are multi-threaded, which means that only one instance of each process runs regardless of how many people use it. It also means that the application itself runs better on servers with more than one processor, as the total of all the users may be divided among all of the processors in the sensor server.

While the above detailed description has shown, described, and pointed out the fundamental novel features of the invention as applied to various embodiments, it will be understood that various omissions and substitutions and changes in the form and details of the system illustrated may be made by those skilled in the art, without departing from the concepts of the invention.

WHAT IS CLAIMED IS:

1. An encrypted remote monitoring system, comprising:

a plurality of remotely located sensor networks, each one of the remotely located sensor networks comprising a plurality of sensors providing sensor data;

a plurality of remotely located sensor monitors, each one of the remotely located sensor monitors being capable of selectively accessing the sensor data of at least one of the sensors located at a selected one of the remotely located sensor networks; and

a centralized sensor computing environment having a first set of connections to the plurality of remotely located sensor networks and a second set of connections to the plurality of remotely located sensor monitors, wherein the first set of connections and the second set of connections form an encrypted virtual private network in a public packet switched network.

2. The system of Claim 1, wherein the first set of connections of the encrypted virtual private network communicate data encrypted by a 168-bit triple data encryption standard (DES).

3. The system of Claim 1, wherein the second set of connections of the encrypted virtual private network communicate data encrypted by a 128-bit secure sockets layer (SSL).

4. The system of Claim 1, wherein one of the remotely located sensor monitors executes a World Wide Web browser.

5. The system of Claim 4, wherein the browser is capable of executing a server push protocol.

6. The system of Claim 4, wherein the browser is capable of executing an applet.

7. The system of Claim 1, wherein at least one of the sensors comprises a video camera.

8. The system of Claim 1, wherein the centralized sensor computing environment comprises a plurality of computers interconnected by a data network.

9. The system of Claim 8, wherein one of the computers comprises a web server, the web server communicating a system web page to the public packet switched network.

10. The system of Claim 9, wherein the web server requests a user password and a center identification code so as to automatically permit access to a secure portion of the system web page.

11. The system of Claim 1, wherein at least one of the remotely located sensor networks includes a remote sensor computing device, wherein the remote sensor computing device has no secondary data storage device.

12. The system of Claim 11, wherein the only input/output devices included in the remote sensor computing device are for data communication with the remote sensors and the first set of connections.

13. The system of Claim 11, wherein the remote sensor computing device excludes an input/output device for communicating data directly to a human being.

14. The system of Claim 13, wherein the excluded input/output device is a keyboard or a video display device.

15. A method of remote monitoring in a system including a centralized server, a plurality of remotely located sensor networks, each network comprising a plurality of sensors, and a plurality of remotely located sensor monitors, the method comprising:

providing sensor data from at least one of the sensors;

communicating the sensor data via an encrypted virtual private network in a public packet switched network to the centralized sensor server;

storing the sensor data in the centralized sensor server; and

selectively accessing the stored sensor data by at least one of the plurality of remotely located sensor monitors via the encrypted virtual private network.

16. The method defined in Claim 15, additionally comprising displaying the accessed sensor data to a user.

17. The method defined in Claim 15, additionally comprising selecting a particular sensor to provide the sensor data.

18. The method defined in Claim 17, wherein the selecting includes selecting a sensor link on a browser located at the at least one of the remotely located sensor monitors.

19. The method defined in Claim 18, additionally comprising requesting a user name, password and a center identification code to permit access to a secure portion of a system web page.

20. The method defined in Claim 15, wherein at least one of the sensors comprises a video camera.

21. An image sharing system, comprising:

a plurality of image sensors, each sensor being capable of providing a unique sequence of images;

a plurality of client computing devices, each client computing device being capable of receiving at least one of the unique sequence of images;

an image fetch program in data communication with a selected one of the image sensors, the image fetch program being capable of fetching each one of the images in the image sequence from the selected image sensor; and

an image distribution program in data communication with the image fetch program, the image distribution program being capable of distributing the image sequence to selected ones of the client computing devices, wherein the image sequence associated with the selected image sensor is shareably accessed by the selected ones of the computing devices.

22. The system defined in Claim 21, wherein the client computing device includes a browser program.

23. The system defined in Claim 21, wherein the image fetch program stores each one of the images of the image sequence in a storage medium and the image distribution program retrieves each one of the images of the image sequence from the storage medium.

24. The system defined in Claim 21, wherein the image fetch and image distribution programs are executed on a computer network, the network residing in a public packet switched network and connected to the image sensors and client computing devices.

25. The system defined in Claim 24, wherein the system additionally comprises a web server intermittently connected to at least one of the client computing devices by the public packet switched network.

26. The system defined in Claim 24, wherein the computer network comprises an encrypted virtual private network in the public packet switched network.

27. An image sharing system, comprising:

a plurality of image sensors, each sensor being capable of providing a unique sequence of images;

a plurality of client computing devices, each client computing device being capable of receiving at least one of the unique sequence of images;

an image server in data communication with a selected image sensor, the image server being capable of generating a sensor thread so as to fetch each one of the images in the image sequence from the selected image sensor; and

a distribution server in data communication with an image output of the sensor thread, the distribution server being capable of generating a client data stream for access by a selected client computing device, wherein the image sequence is shared with respect to the selected image sensor by more than one of the client computing devices.

28. The system defined in Claim 27, wherein the client computing device includes a browser program.

29. The system defined in Claim 27, wherein the image server stores each of the fetched images of the image sequence in a storage medium.

30. The system defined in Claim 29, wherein the distribution server retrieves each of the fetched images of the image sequence from the storage medium.

31. The system defined in Claim 30, wherein the distribution server sends the obtained image to the selected client computing device.

32. The system defined in Claim 27, wherein the image fetch and image distribution programs are executed on a computer network, the network residing in a public packet switched network and connected to the image sensors and client computing devices.

33. The system defined in Claim 32, wherein the system additionally comprises a web server intermittently connected to at least one of the client computing devices by the public packet switched network.

34. The system defined in Claim 32, wherein the computer network comprises an encrypted virtual private network in the public packet switched network.

35. A method of sharing images in a remote monitoring system including a plurality of image sensors and a plurality of client computing devices, the method comprising:

providing a unique sequence of images associated with a selected one of the image sensors;

fetching each one of the images in the image sequence from the selected image sensor; and

distributing the image sequence to selected ones of the client computing devices, wherein the image sequence associated with the selected image sensor is shareably accessed by the selected ones of the client computing devices.

36. The method defined in Claim 35, additionally comprising displaying the distributed image sequence at at least one of the selected client computing devices.

37. The method defined in Claim 35, wherein at least one of the image sensors comprises a video camera.

38. The method defined in Claim 35, additionally comprising identifying one of the selected image sensors by use of a browser located at the selected client computing device.

39. The method defined in Claim 35, additionally comprising storing the fetched images of the image sequence in a storage medium.

40. The method defined in Claim 39, additionally comprising retrieving the stored images for the distributing.

41. The method defined in Claim 35, additionally comprising non-persistently interconnecting the image sensors and the client computing devices by an encrypted virtual private network in a public packet switched network.

42. A method of sharing images in a remote monitoring system including a plurality of image sensors and a plurality of client computing devices, the method comprising:

providing a unique sequence of images associated with a selected image sensor;

retrieving each one of the images in the image sequence from the selected image sensor with a sensor thread;

storing the retrieved images of the image sequence in a storage medium; and

retrieving the image sequence into a client data stream for shareable accessing the image sequence by selected ones of the client computing devices.

43. The method defined in Claim 42, additionally comprising receiving at least one of the unique sequence of images at the selected client computing device from the storage medium.

44. The method defined in Claim 42, additionally comprising sending the client data stream to the selected client computing devices.

45. The method defined in Claim 42, additionally comprising identifying one of the selected image sensors by use of a browser located at the selected client computing device.

46. The method defined in Claim 42, additionally comprising interconnecting the image sensors and the client computing devices by an encrypted virtual private network in a public packet switched network.

47. A method of providing security for a system having a standardized transport protocol server in data communication with a database containing authorized user identification information and a user browser, the method comprising:

sending a set of connection state data indicative of an authorized user data from a standardized transport protocol server to a user browser corresponding with the authorized user;

sending the user connection state data to the standardized transport protocol server when the authorized user selects a link to a secure area of a hyperlinked page;

comparing the user connection state data to corresponding connection state data in the database; and

granting access to the secure area by the authorized user if the comparison result indicates that the authorized user is permitted to access the secure area.

48. The method defined in Claim 47, wherein the granting includes sending data from the secure area to the authorized user.

49. The method defined in Claim 47, additionally comprising:

determining if the user has been inactive in the hyperlinked page for a predetermined time interval; and

terminating user access if the time interval has been exceeded.

50. The method defined in Claim 49, additionally comprising sending secure data to the user browser if the time interval has not been exceeded.

51. The method defined in Claim 47, additionally comprising:

presenting the system hyperlinked page to the user browser corresponding with a particular user;

requesting a user login name, a user password and an organization identification code from the particular user; and

authorizing the user if the user login name, the user password and the organization identification code match corresponding data in the database.

52. The method defined in Claim 47, wherein the set of connection state data comprises an Internet cookie.

53. The method defined in Claim 47, wherein the connection state data comprises one or more of organization identification, account identification, child account identification, browser identification, unique random code, and expiration date.

54. A security system for a web application, comprising:

a web server being capable of sending a web page having at least one secure area;

a web database in data communication with the web server, wherein the web database stores connection state data for a plurality of users;

a client computing device running a user browser, the user browser being capable of receiving connection state data corresponding to an authorized user from the web server and sending the user's connection state data to the web server when the authorized user selects a link to the secure area of the web page;

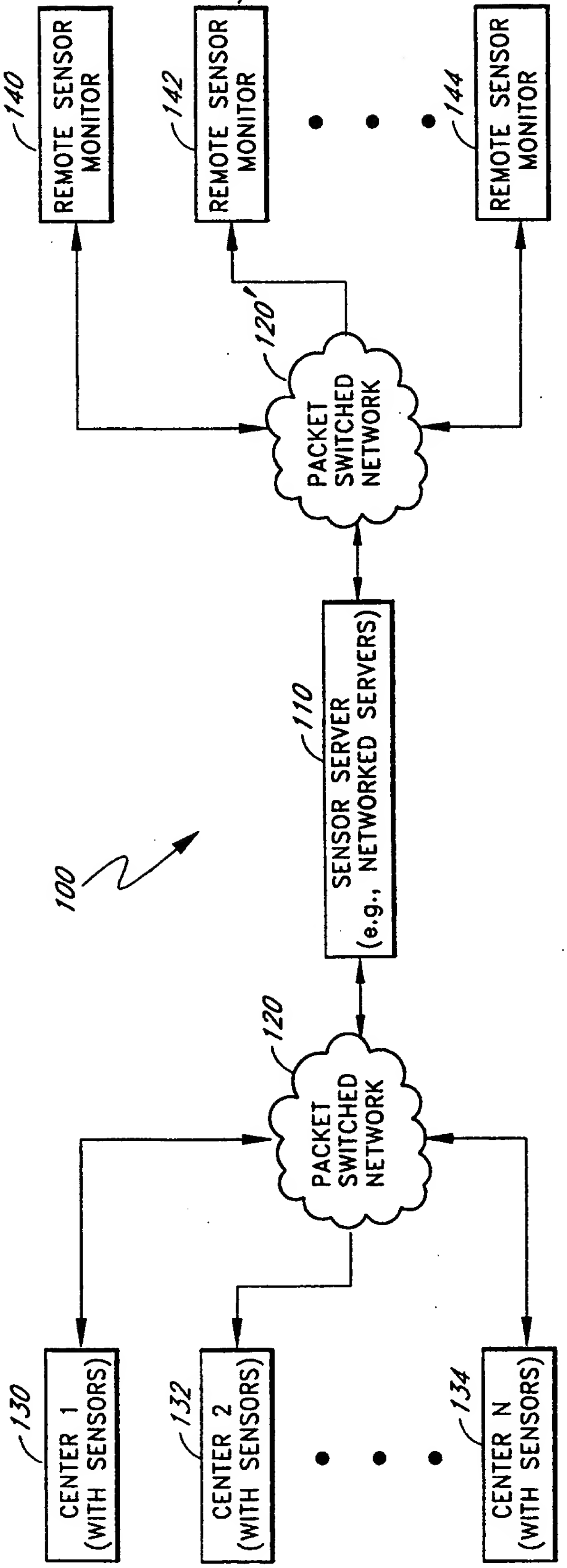
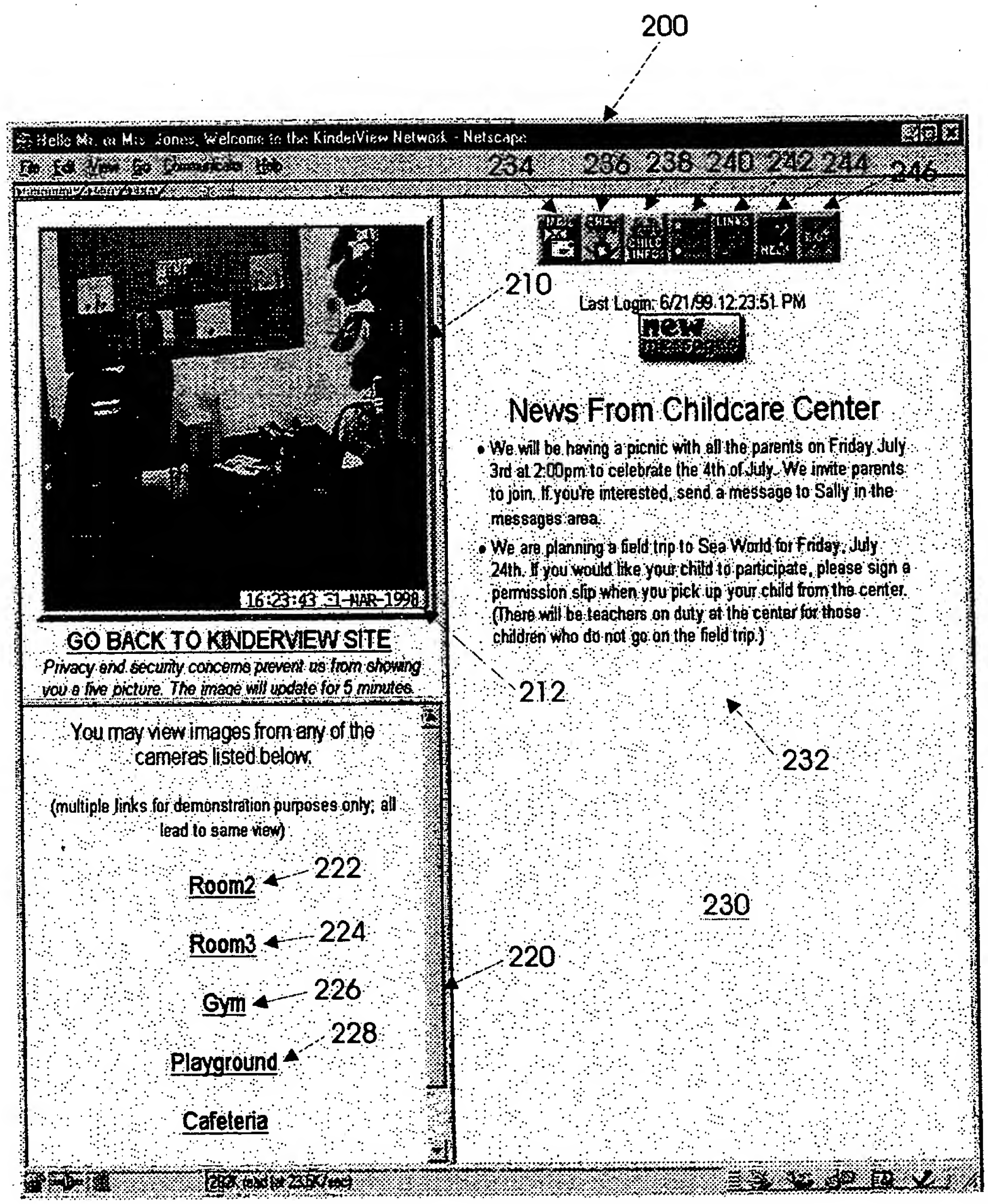

100
REMOTE SENSOR MONITOR
140
REMOTE SENSOR MONITOR
142
REMOTE SENSOR MONITOR
144
120'
PACKET SWITCHED NETWORK
SENSOR SERVER (e.g., NETWORKED SERVERS)
110
120
PACKET SWITCHED NETWORK
CENTER 1 (WITH SENSORS)
130
CENTER 2 (WITH SENSORS)
132
CENTER N (WITH SENSORS)
134

FIG. 1


200
Hello Mr. or Mrs. Jones, Welcome to the KinderView Network - Netscape
File Edit View Go Communicator Help
234
236
238
240
242
244
246
LINKS
CHILD INFO
HELP
210
212
16:23:43 31-MAR-1998
new messages
232
230
220
222
224
226
228

Last Login: 6/21/99 12:23:51 PM

News From Childcare Center

- We will be having a picnic with all the parents on Friday July 3rd at 2:00pm to celebrate the 4th of July. We invite parents to join. If you're interested, send a message to Sally in the messages area.
- We are planning a field trip to Sea World for Friday, July 24th. If you would like your child to participate, please sign a permission slip when you pick up your child from the center. (There will be teachers on duty at the center for those children who do not go on the field trip.)

GO BACK TO KINDERVIEW SITE

Privacy and security concerns prevent us from showing you a live picture. The image will update for 5 minutes.

You may view images from any of the cameras listed below.

(multiple links for demonstration purposes only; all lead to same view)

Room2

Room3

Gym

Playground

Cafeteria

FIG.2

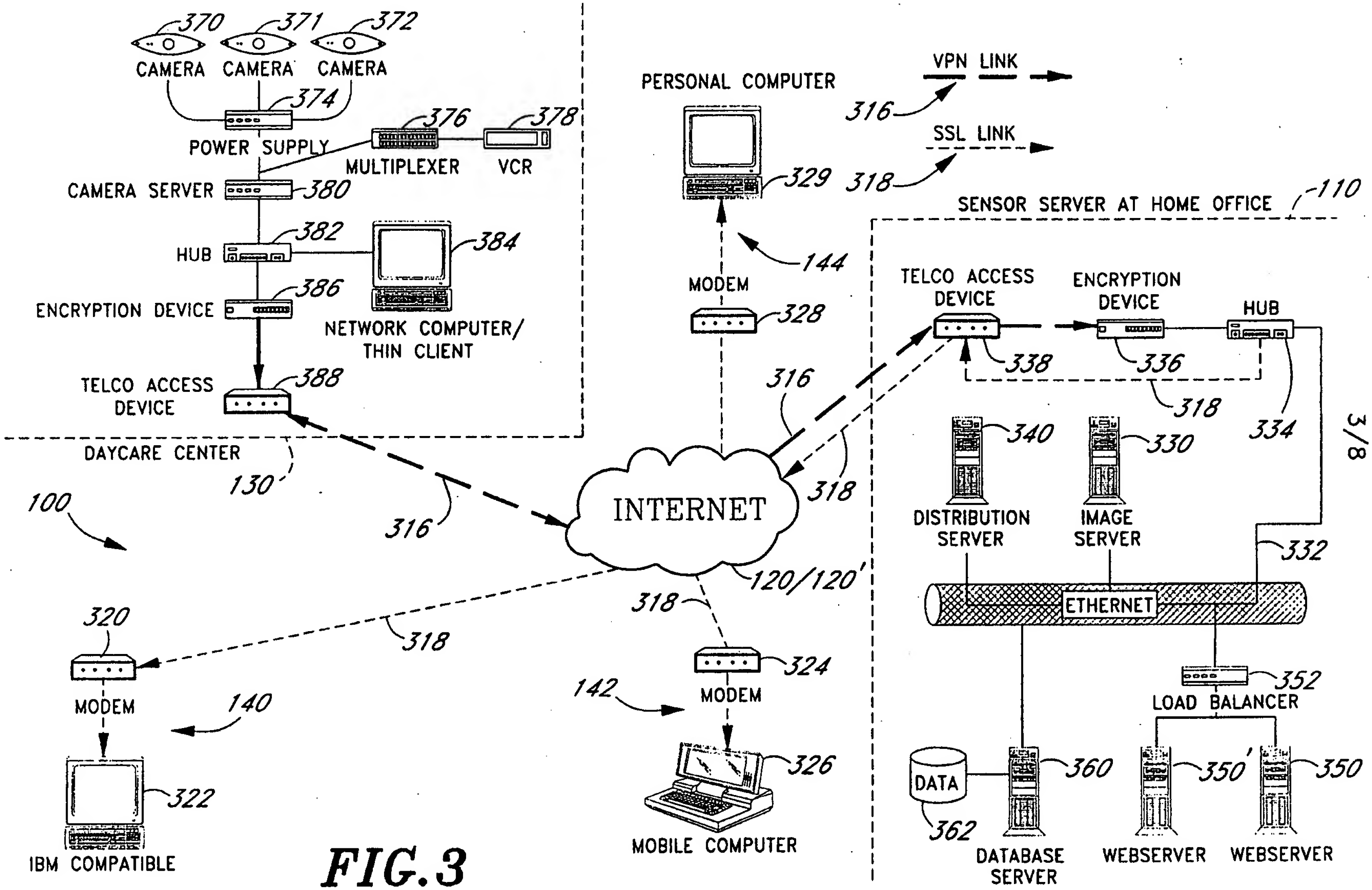

370
371
372
CAMERA
CAMERA
CAMERA
374
POWER SUPPLY
376
378
MULTIPLEXER
VCR
CAMERA SERVER
380
HUB
382
384
ENCRYPTION DEVICE
386
NETWORK COMPUTER/
THIN CLIENT
TELCO ACCESS
DEVICE
388
DAYCARE CENTER
130
100
316
PERSONAL COMPUTER
329
144
MODEM
328
316
VPN LINK
318
SSL LINK
SENSOR SERVER AT HOME OFFICE
110
TELCO ACCESS
DEVICE
338
ENCRYPTION
DEVICE
336
HUB
334
318
316
318
INTERNET
120/120'
340
DISTRIBUTION
SERVER
330
IMAGE
SERVER
332
ETHERNET
352
LOAD BALANCER
DATA
362
360
DATABASE
SERVER
350'
WEBSERVER
350
WEBSERVER
320
MODEM
318
140
322
IBM COMPATIBLE
318
324
MODEM
142
326
MOBILE COMPUTER

FIG.3

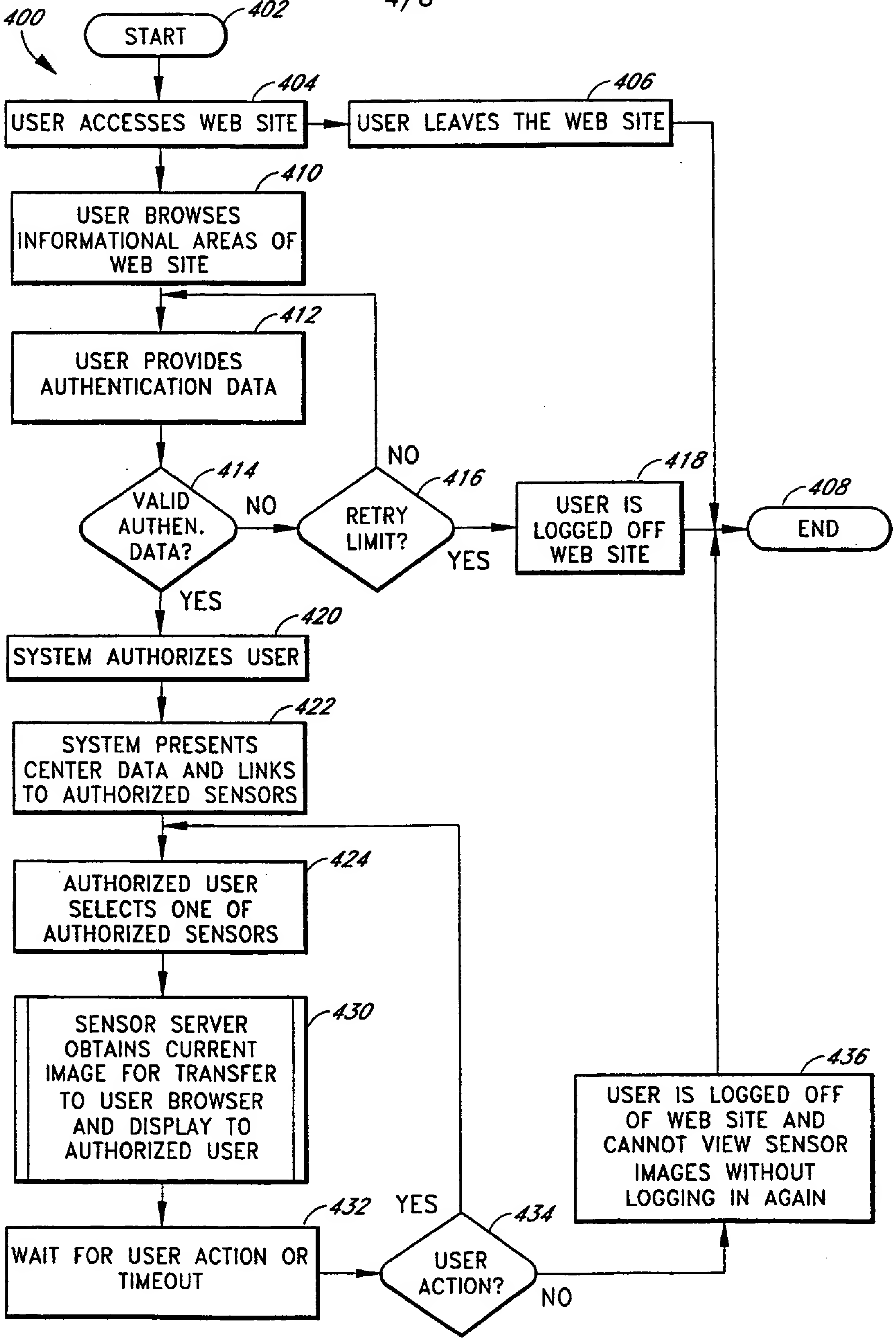
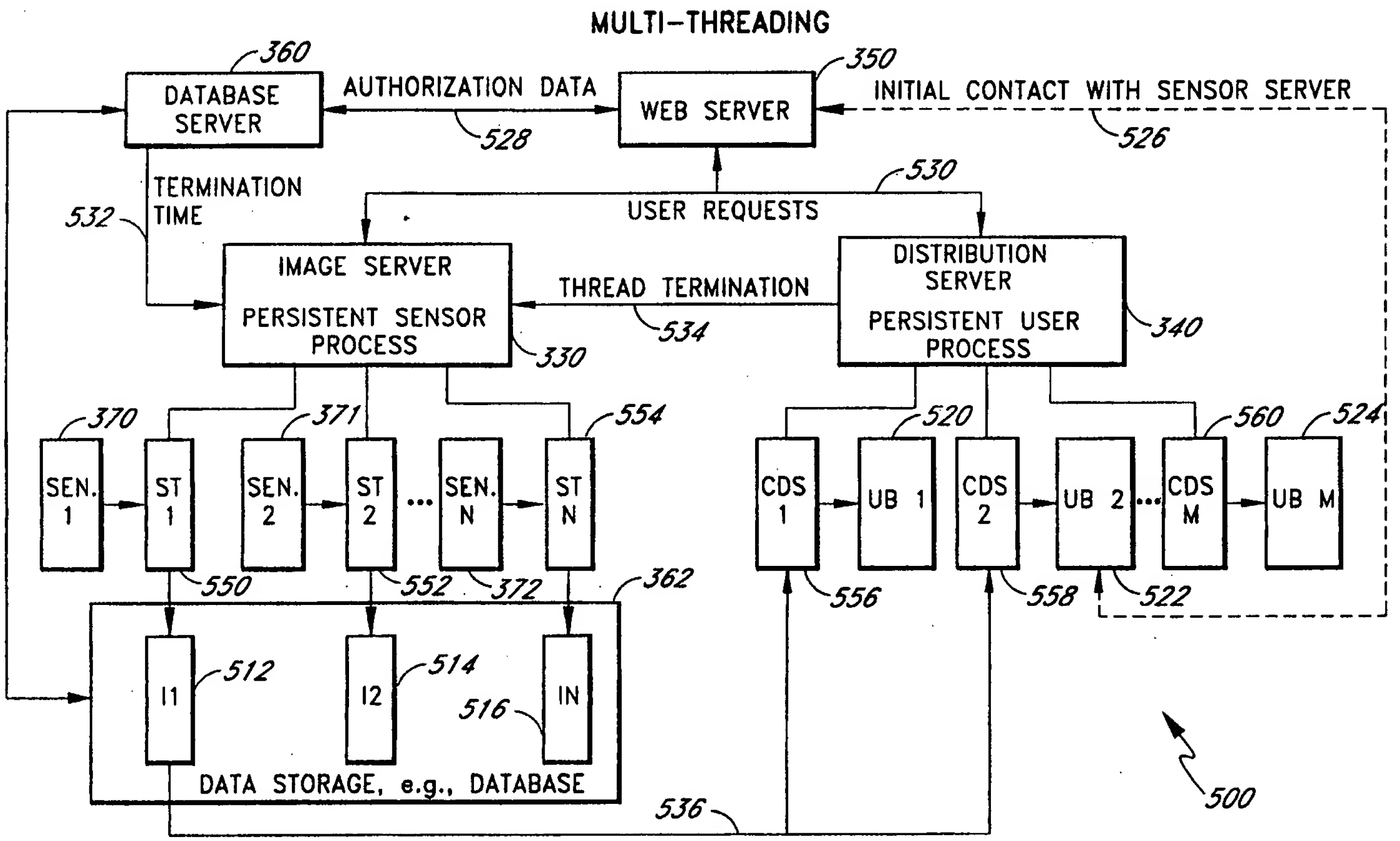

400
START
402
USER ACCESSES WEB SITE
404
USER LEAVES THE WEB SITE
406
USER BROWSES INFORMATIONAL AREAS OF WEB SITE
410
USER PROVIDES AUTHENTICATION DATA
412
VALID AUTHEN. DATA?
414
NO
RETRY LIMIT?
416
NO
YES
USER IS LOGGED OFF WEB SITE
418
END
408
YES
SYSTEM AUTHORIZES USER
420
SYSTEM PRESENTS CENTER DATA AND LINKS TO AUTHORIZED SENSORS
422
AUTHORIZED USER SELECTS ONE OF AUTHORIZED SENSORS
424
SENSOR SERVER OBTAINS CURRENT IMAGE FOR TRANSFER TO USER BROWSER AND DISPLAY TO AUTHORIZED USER
430
USER IS LOGGED OFF OF WEB SITE AND CANNOT VIEW SENSOR IMAGES WITHOUT LOGGING IN AGAIN
436
WAIT FOR USER ACTION OR TIMEOUT
432
YES
USER ACTION?
434
NO

FIG.4



SEN=SENSOR AT REMOTE LOCATION(E.G., DAY CARE CENTER)
ST=SENSOR THREAD
I=IMAGE(S)
CDS=CLIENT DATA STREAM
UB=USER BROWSER AT REMOTE LOCATION (E.G., USER'S BUSINESS)

FIG.5

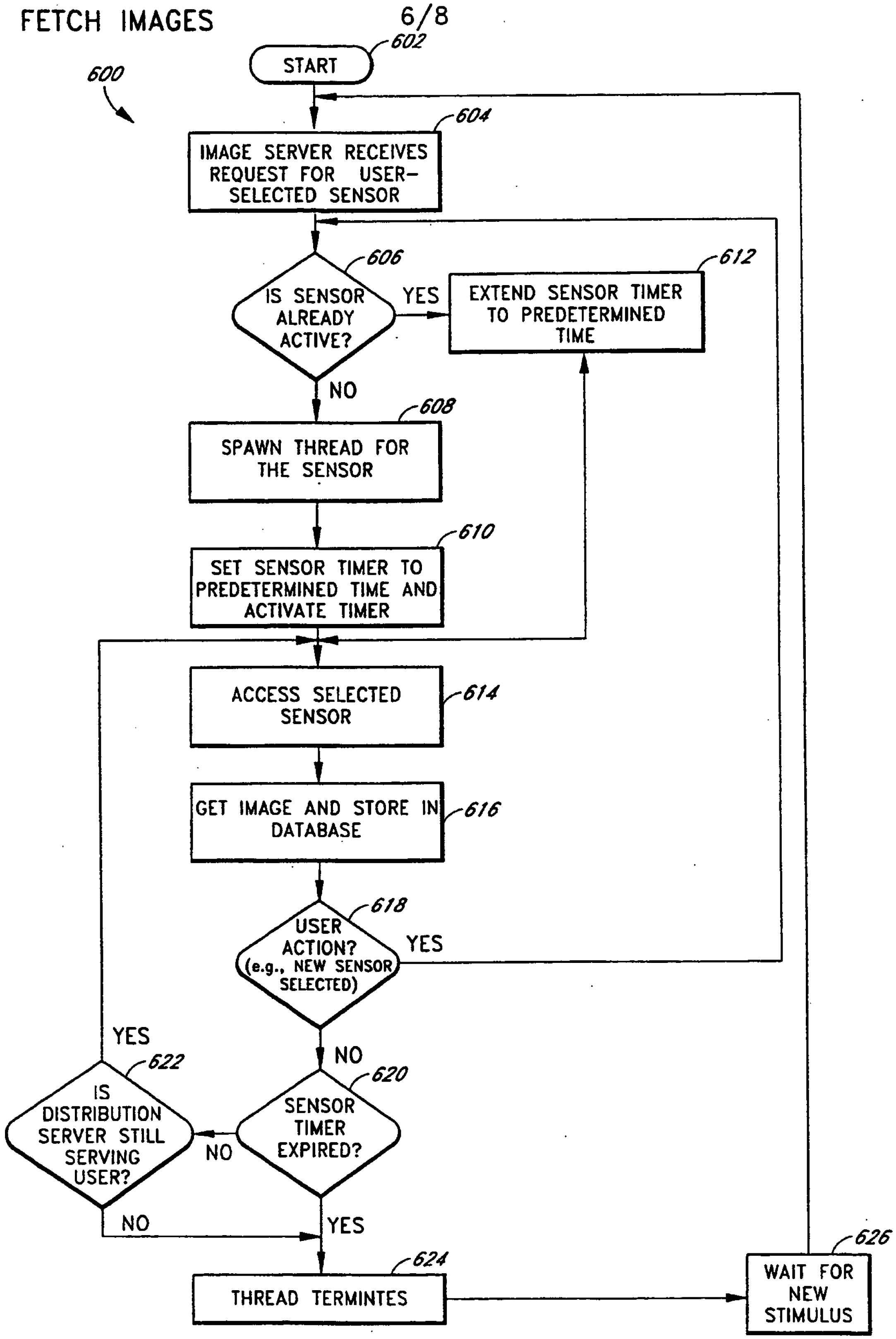

FETCH IMAGES
600
START
602
IMAGE SERVER RECEIVES REQUEST FOR USER-SELECTED SENSOR
604
IS SENSOR ALREADY ACTIVE?
606
YES
EXTEND SENSOR TIMER TO PREDETERMINED TIME
612
NO
SPAWN THREAD FOR THE SENSOR
608
SET SENSOR TIMER TO PREDETERMINED TIME AND ACTIVATE TIMER
610
ACCESS SELECTED SENSOR
614
GET IMAGE AND STORE IN DATABASE
616
USER ACTION? (e.g., NEW SENSOR SELECTED)
618
YES
NO
SENSOR TIMER EXPIRED?
620
NO
IS DISTRIBUTION SERVER STILL SERVING USER?
622
YES
NO
YES
THREAD TERMINTES
624
WAIT FOR NEW STIMULUS
626

FIG.6

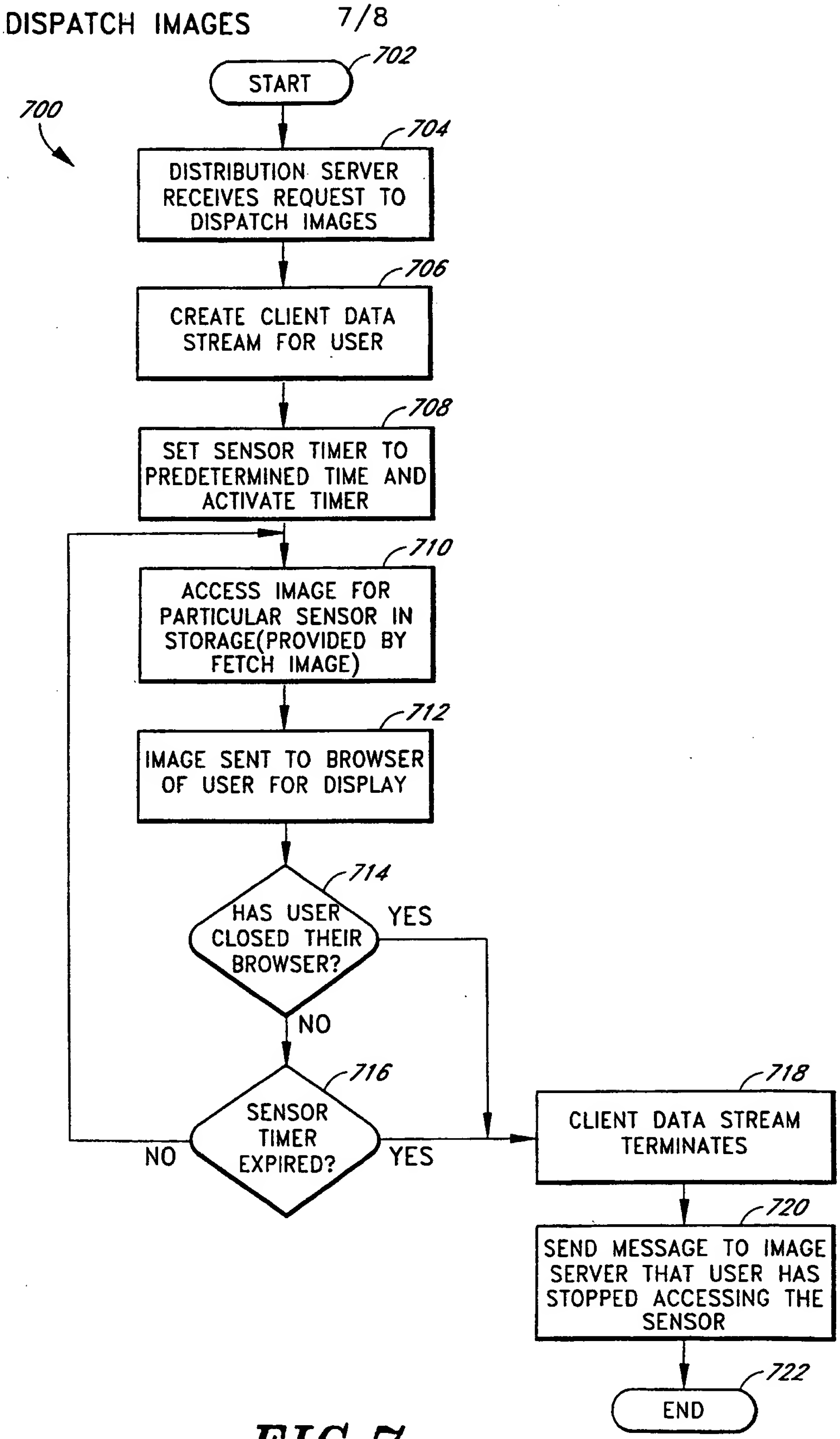

DISPATCH IMAGES
700
702
START
704
DISTRIBUTION SERVER RECEIVES REQUEST TO DISPATCH IMAGES
706
CREATE CLIENT DATA STREAM FOR USER
708
SET SENSOR TIMER TO PREDETERMINED TIME AND ACTIVATE TIMER
710
ACCESS IMAGE FOR PARTICULAR SENSOR IN STORAGE(PROVIDED BY FETCH IMAGE)
712
IMAGE SENT TO BROWSER OF USER FOR DISPLAY
714
HAS USER CLOSED THEIR BROWSER?
YES
NO
716
SENSOR TIMER EXPIRED?
NO
YES
718
CLIENT DATA STREAM TERMINATES
720
SEND MESSAGE TO IMAGE SERVER THAT USER HAS STOPPED ACCESSING THE SENSOR
722
END

FIG.7

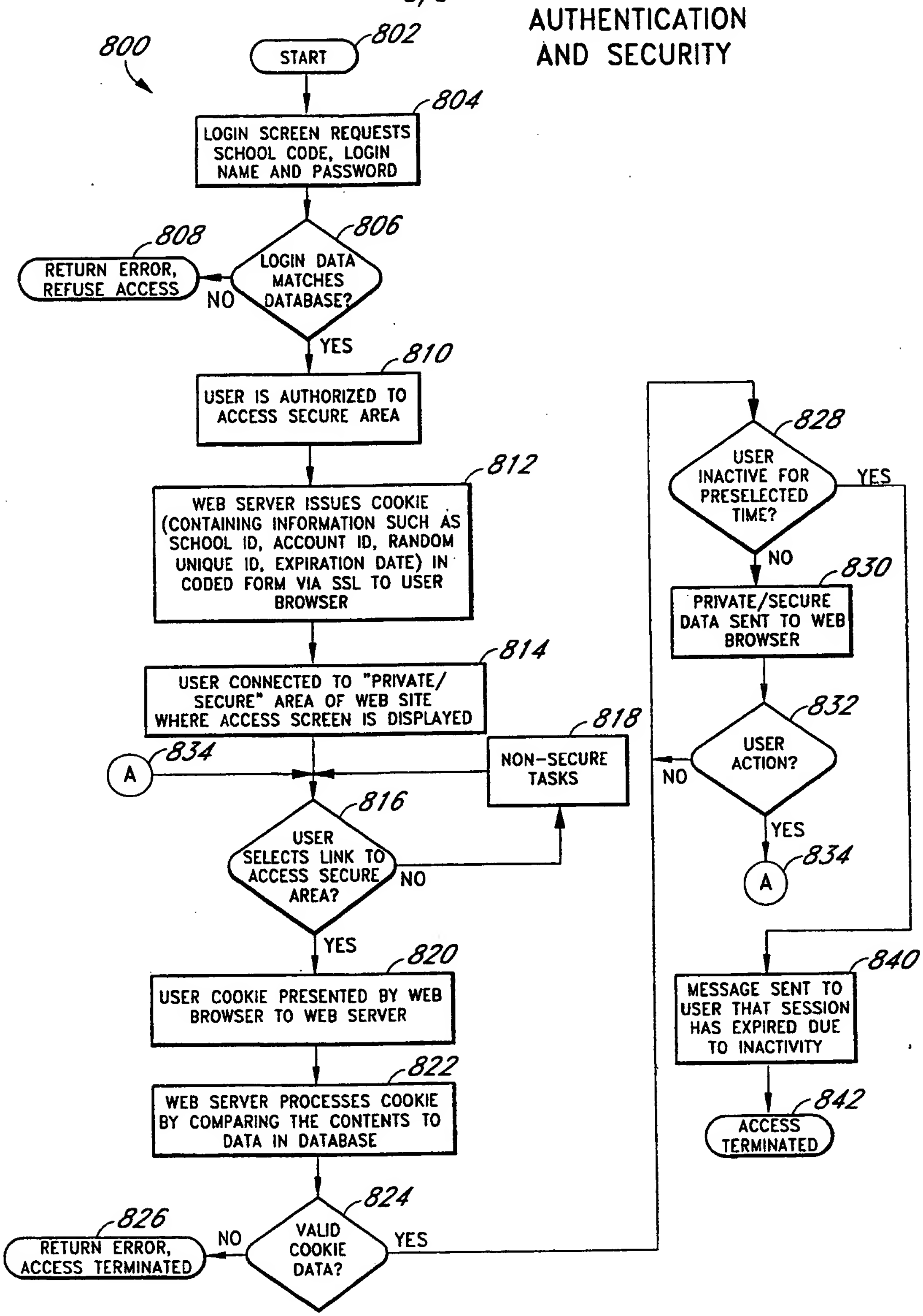

AUTHENTICATION AND SECURITY
800
START
802
LOGIN SCREEN REQUESTS SCHOOL CODE, LOGIN NAME AND PASSWORD
804
LOGIN DATA MATCHES DATABASE?
806
NO
RETURN ERROR, REFUSE ACCESS
808
YES
USER IS AUTHORIZED TO ACCESS SECURE AREA
810
WEB SERVER ISSUES COOKIE (CONTAINING INFORMATION SUCH AS SCHOOL ID, ACCOUNT ID, RANDOM UNIQUE ID, EXPIRATION DATE) IN CODED FORM VIA SSL TO USER BROWSER
812
USER CONNECTED TO "PRIVATE/ SECURE" AREA OF WEB SITE WHERE ACCESS SCREEN IS DISPLAYED
814
A
834
NON-SECURE TASKS
818
USER SELECTS LINK TO ACCESS SECURE AREA?
816
NO
YES
USER COOKIE PRESENTED BY WEB BROWSER TO WEB SERVER
820
WEB SERVER PROCESSES COOKIE BY COMPARING THE CONTENTS TO DATA IN DATABASE
822
VALID COOKIE DATA?
824
NO
RETURN ERROR, ACCESS TERMINATED
826
YES
USER INACTIVE FOR PRESELECTED TIME?
828
YES
NO
PRIVATE/SECURE DATA SENT TO WEB BROWSER
830
USER ACTION?
832
NO
YES
A
834
MESSAGE SENT TO USER THAT SESSION HAS EXPIRED DUE TO INACTIVITY
840
ACCESS TERMINATED
842

FIG.8

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 June 2000 (22.06.2000)

PCT

(10) International Publication Number
WO 00/36807 A3

(51) International Patent Classification⁷: H04L 29/06

(21) International Application Number: PCT/US99/30139

(22) International Filing Date:
17 December 1999 (17.12.1999)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/216,388	18 December 1998 (18.12.1998)	US
09/216,415	18 December 1998 (18.12.1998)	US
09/216,700	18 December 1998 (18.12.1998)	US

(71) Applicant: CYBERSIGNS, INC. [US/US]; Suite 202, 8304 Clairemont Mesa Boulevard, San Diego, CA 92111 (US).

(72) Inventors: BOODMAN, David, J.; 4271 Calle Mar De Ballenas, San Diego, CA 92130 (US). FURMAN, Adam; 11517 Windcrest Lane #38, San Diego, CA 92128 (US). KOZUBIK, John; P.O. Box 4867, Boulder, CO 80306 (US). CHIRANAKHON, Grean; Apt. 183, 3770 Boyd Avenue, San Diego, CA 92111 (US).

(74) Agent: HUNT, Dale, C.; Knobbe, Martens, Olson & Bear, LLP, 16th floor, 620 Newport Center Drive, Newport Beach, CA 92660 (US).

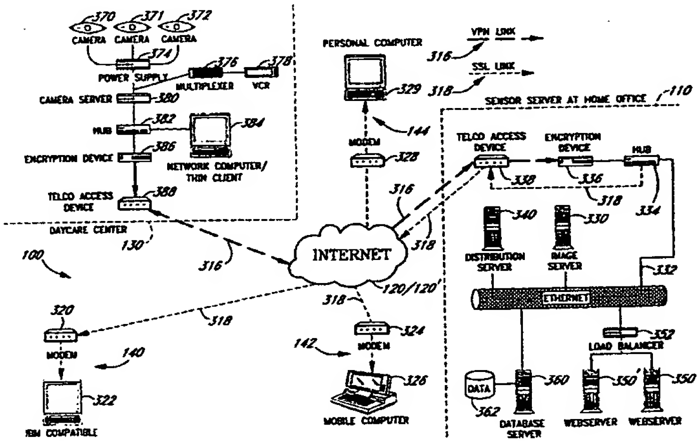
(81) Designated States (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

[Continued on next page]

(54) Title: ENCRYPTED VIRTUAL PRIVATE NETWORK FOR ACCESSING REMOTE SENSORS



(57) Abstract: One aspect of the present invention is directed to a system and method of providing secure access to remote sensor data via an encrypted virtual private network (316). The system (100) utilizes a scaleable architecture and includes a centralized sensor server (110) connected to a plurality of centers (130, 132, 134) having sensors (370, 371, 372) via an encrypted virtual private network. The centralized server also connects to a plurality of remote sensor monitors (140, 142, 144) via a virtual private network. The virtual private network may be implemented over a packet switched network (120) such as the Internet, while the remote sensor monitor utilizes a web browser (520, 522, 524). The system shares images (512) from a particular sensor to multiple users via the centralized server to conserve bandwidth and reduce system costs. The system utilizes various authentication and security features to protect the sensor data.

(88) Date of publication of the international search report: 21 December 2000

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/30139

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 0 964 568 A (CIT ALCATEL) 15 December 1999 (1999-12-15) column 2, line 22 - line 35 column 2, line 57 -column 3, line 9 column 3, line 35 - line 39 column 8, line 36 - line 51	1,15
A		2-14, 16-46

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search
8 June 2000

Date of mailing of the international search report
16. 10. 2000

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
Tous Fajardo, J

2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/30139

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SCHMIDT M: "UNTER AUSSCHLUSS DER OEFFENTLICHKEIT VIRTUAL PRIVATE NETWORKS - VERTRAULICHER DATENAUSTAUSCH UEBER DAS INTERNET" CT MAGAZIN FUER COMPUTER TECHNIK,DE,VERLAG HEINZ HEISE GMBH., HANNOVER, no. 8, 14 April 1998 (1998-04-14), pages 226-230,232-23, XP000741250 ISSN: 0724-8679 * The whole document * ---	1-3,15, 21,27, 35,42
A	WUNNAVA S V ET AL: "Advances in virtual design and virtual center concepts" PROCEEDINGS OF IEEE SOUTHEASTON '96. BRINGING TOGETHER EDUCATION, SCIENCE AND TECHNOLOGY, TAMPA, FL, USA, 11 - 14 April 1996, pages 107-110, XP002139667 ISBN: 0-7803-3088-9 page 107, column 1, line 14 - line 19 page 108, column 1, line 19 - line 22 page 110, column 1, line 32 -column 2, line 20 figures 2,6 ---	1,15,21, 27,35,42
A	DE ALBUQUERQUE M P ET AL: "Remote monitoring over the Internet" NUCLEAR INSTRUMENTS & METHODS IN PHYSICS RESEARCH, SECTION - A: ACCELERATORS, SPECTROMETERS, DETECTORS AND ASSOCIATED EQUIPMENT,NL,NORTH-HOLLAND PUBLISHING COMPANY. AMSTERDAM, vol. 412, no. 1, 21 July 1998 (1998-07-21), pages 140-145, XP004131956 ISSN: 0168-9002 * The whole document * ---	1,15,21, 27,35,42
A	GABEL J: "UEBERMITTLUNG VON FERNWIRKINFORMATIONEN MIT TEMEX" ELEKTROTECHNISCHE ZEITSCHRIFT - ETZ,DE,VDE VERLAG GMBH. BERLIN, vol. 105, no. 20, 1 October 1984 (1984-10-01), pages 1088-1091, XP002033566 ISSN: 0948-7387 page 1088, column 2, line 3 -column 3, line 7 page 1089, column 1, line 3 - line 9 page 1089, column 3, line 10 - line 20 figure 2 ---	1,15,21, 27,35,42
	-/--	

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/30139

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 717 379 A (PETERS WOLFGANG) 10 February 1998 (1998-02-10) column 1, line 59 -column 2, line 20 column 3, line 18 - line 30 column 3, line 60 -column 4, line 3 column 5, line 11 - line 23 column 5, line 38 - line 42 ———	1-46

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 99/30139

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. □ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. □ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. □ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. □ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-46

Remark on Protest

□ The additional search fees were accompanied by the applicant's protest.

□ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

1. Claims: 1-46

Encrypted remote monitoring system and method in a secure virtual private network comprising a centralized sensor computer environment.

2. Claims: 47-58

Method and system for providing secure web applications comprising a web server being capable of sending a web page having at least one secure area.

INTERNATIONAL SEARCH REPORT

Information on patent family members

ternational Application No
PCT/US 99/30139

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0964568 A	15-12-1999	DE 19826087 A	23-12-1999
US 5717379 A	10-02-1998	DE 19512959 A EP 0738065 A JP 9016685 A	17-10-1996 16-10-1996 17-01-1997